



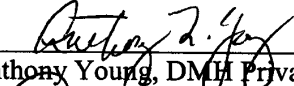
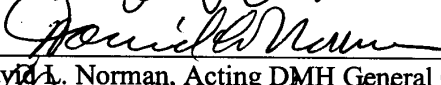
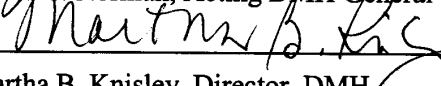
## DEPARTMENT OF MENTAL HEALTH

### PRIVACY POLICIES & PROCEDURES

These DMH Privacy Policies and Procedures implement our obligations to protect the privacy of individually identifiable health information that we as Network participants create, receive or maintain in our respective roles as health care providers or as a health plan. We implement these DMH Privacy Policies and Procedures as a matter of sound business practice, to protect the interests of our consumers, and to fulfill our legal obligations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations at 45 Code of Federal Regulations Parts 160 and 164 ("Privacy Rules"). In this manual, the HIPAA requirements have been merged, as appropriate, with the requirements of the D.C. Mental Health Information Act (MHIA) of 1978 so that we can also continue to meet our obligations to our consumers under that Act.

As a member of our workforce, you are obligated to follow these DMH Privacy Policies and Procedures faithfully. Failure to comply with these policies would subject DMH employees to discipline in accordance with Chapter 16 of the DPM and applicable collective bargaining agreements. All workforce members (including DMH employees) are subject to civil and criminal penalties for violation HIPAA and the MHIA.

If you have questions about any use or disclosure of individually identifiable health information or about your obligations under these DMH Privacy Policies and Procedures, the HIPAA Privacy Rules or other federal or state law, consult your Privacy Officer, or the DMH Privacy Officer, Anthony Young, at the DC Department of Mental Health, 64 New York Ave., NE, 4<sup>th</sup> Floor, Washington, D.C. 20002, telephone (202) 673-2200, Fax: (202) 673-3433, TTD/TTY: (202) 673-7500, E-mail: [dmh.privacy@dc.gov](mailto:dmh.privacy@dc.gov). In addition, DMH employees can also contact the District Privacy Official, Gerry Roth, at 1350 Pennsylvania Ave, NW, Suite 307, Washington, DC 20004, telephone: (202) 727-8001, Fax: (202) 727-0246, or email: [dcprivacy@dc.gov](mailto:dcprivacy@dc.gov), before you act.

 Anthony Young, DMH Privacy Officer	7/16/03 (Date)
 David L. Norman, Acting DMH General Counsel	7/16/03 (Date)
 Martha B. Knisley, Director, DMH	7/16/03 (Date)

Department of Mental Health  
**TRANSMITTAL LETTER**

SUBJECT		
DMH Privacy Policies and Procedures		
POLICY NUMBER	DATE	TL#
DMH Policy 645.1	JUL 16 2003	28

**Purpose.** To implement guidelines and procedures consistent with federal and District law that protect the privacy of our consumers' health information. The governing privacy guidelines are described in this policy. Specific topics and procedures are addressed in the Department of Mental Health (DMH) Privacy Policies and Procedures Operations Manual. The manual shall be disseminated throughout the Department and made available to Network providers.

**Applicability.** DMH and its participating Network providers.

*Network* means an organized health care arrangement consisting of DMH, and every mental health provider that is certified, licensed, or otherwise regulated by DMH, or has entered into a contract or agreement with DMH for the provision of mental health services or mental health supports.

This policy replaces any requirements in existing Department policies that may contain different information relating to confidentiality of mental health information. Those policies shall be revised accordingly.

**Policy Clearance.** Reviewed by affected responsible staff, including DMH General Counsel, DMH, CSA and SEH Privacy Officers and others.

**Implementation Plans.** A plan of action to implement or adhere to this policy must be developed by designated responsible staff. If materials and/or training are required to implement this policy, these requirements must be part of the action plan. Specific staff should be designated to carry out the implementation and program managers are responsible for following through to ensure compliance. Action plans and completion dates should be sent to the appropriate authority. Contracting Officer Technical Representatives (COTRs) must also ensure that contractors are informed of this policy if it is applicable or pertinent to their scope of work. *Implementation of all DMH policies shall begin as soon as possible. Full implementation of this policy shall be completed within sixty (60) days after the date of this policy.*

**Policy Dissemination and Filing Instructions.** Managers/supervisors of DMH and DMH contractors must ensure that staff are informed of this policy. Each staff person who maintains policy manuals must promptly file this policy in Volume I of the blue **DMH** Policy and Procedures Manual, and contractors must ensure that this policy is maintained in accordance with their internal procedures. *A copy of this policy must also remain in the Privacy Policies and Procedures Operations Manual, which must be located in all programs that use and disclose PHI (See Section 13 of the policy).*

(See Back)

\*If any CMHS or DMH policies are referenced in this policy, copies may be obtained from the DMH Policy Support Division by calling (202) 673-7757.

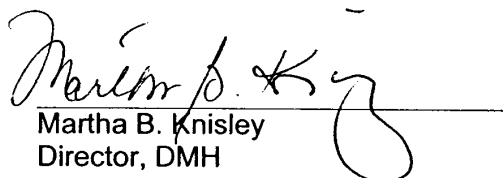
**ACTION**


**REMOVE AND DESTROY**

**CMHS 50000.645.1  
(dated September 8, 1988)**

**INSERT**

**DMH Policy 645.1, and  
see filing instructions above.**

  
Martha B. Knisley  
Director, DMH

GOVERNMENT OF THE DISTRICT OF COLUMBIA  DEPARTMENT OF MENTAL HEALTH	Policy No. 645.1	Date JUL 16 2003	Page 1
	Supersedes CMHS 50000.645.1, Confidentiality of Records Guidelines, dated September 8, 1988		
Subject: DMH Privacy Policies and Procedures			

1. **Purpose.** To implement guidelines and procedures consistent with federal and District law that protect the privacy of our consumers' health information. The governing privacy guidelines are described in this policy. Specific topics and procedures are addressed in the Department of Mental Health (DMH) Privacy Policies and Procedures Operations Manual (See Section 13 for distribution of this manual).

2. **Applicability.** DMH and its participating Network providers.

*Network* means an organized health care arrangement consisting of DMH, and every mental health provider that is certified, licensed, or otherwise regulated by DMH, or has entered into a contract or agreement with DMH for the provision of mental health services or mental health supports.

This policy replaces any requirements in existing Department policies that may contain different information relating to confidentiality of mental health information. Those policies shall be revised accordingly.

3. **Authority.** Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations at 45 Code of Federal Regulations Parts 160 and 164 ("HIPAA Privacy Rules"), and the District of Columbia Mental Health Information Act of 1978.

4. **Policy.**

4a. It is the policy of DMH to protect the privacy of consumers' health information that DMH and its participating Network providers create, receive or maintain in their respective roles as health care providers.

4b. Each workforce member with access to protected health information (PHI) must, at all times, comply with the policies and procedures set out in the DMH Privacy Policies and Procedures.

4c. Workforce members shall consult with their Privacy Officer or designee before they use or disclose PHI if there is any doubt regarding whether such use or disclosure is permitted by the DMH Privacy Policies and Procedures or by the HIPAA Privacy Rules.

4d. Failure to comply with the DMH privacy policies and procedures may subject DMH employees to discipline in accordance with Chapter 16 of the District Personnel Manual (DPM) and applicable collective bargaining agreements, and all workforce members to potential civil and criminal penalties (See Section 7 below).

4e. Only the DMH Privacy Officer, with approval from the DMH Director and other District approvals as required, may change the DMH Privacy Policies and Procedures.

5. **Privacy Officers, Agency Heads.**

5a. The DMH Privacy Officer is responsible for developing, maintaining, and implementing the DMH Privacy Policies and Procedures, and for overseeing full compliance with the DMH policies and procedures, the HIPAA Privacy Rules, the D.C. Mental Health Information Act and other

applicable federal and state privacy law.

5b. The DMH Privacy Officer shall serve as the Privacy Officer for DMH Authority level employees and as the senior Privacy Officer for the Department. Saint Elizabeths Hospital (SEH) and the DC Community Services Agency (DC CSA) shall have their own Privacy Officer who must also comply with the duties and responsibilities of the Privacy Officer as outlined in the DMH Privacy Policies and Procedures. Other Network providers shall designate personnel and establish systems to carry out the duties of a Privacy Officer as required by HIPAA.

Each Privacy Officer may delegate specific duties and responsibilities to designees who are trained to assist in carrying out the duties of the Privacy Officer. In addition, the Privacy Officers shall consult with their respective legal offices when situations arise that are beyond the scope of their knowledge.

5c. The DMH Director and each agency head shall ensure that the requirements of these policies and procedures are carried out, and that workforce members become familiar with and adhere to these policies and procedures.

5d. *After Regular Work Hours.* DMH Administrators-On-Call shall contact the Privacy Officer on call for their organization if questions regarding use and disclosure of PHI related to an emergency arise after regular working hours. Other Network participants shall also ensure that mechanisms are in place to appropriately address these issues after regular working hours.

## **6. Workforce Training.**

6a. Each workforce member who may have access to or use of PHI shall receive training on the DMH Privacy Policies and Procedures as necessary and appropriate for the member to carry out his or her job functions.

6b. Training Process. The DMH Privacy Officer and Privacy Officers at the DC CSA and SEH shall work with the DMH Training Institute and their respective local training offices, and the DMH Division of Human Resources (DHR) to facilitate training DMH employees, including determining the appropriate training content needed by particular trainees and new hires to carry out their job functions. The DHR Director or designee shall coordinate training of newly hired members of our workforce as promptly as practical, but before the new hires are given access to or use of PHI. Other Network providers must ensure that their workforce members are appropriately trained.

### **6c. Training Timing.**

- (1) Current Workforce. Existing workforce must complete privacy training.
- (2) New Hires. Newly hired members of our workforce must receive privacy training before they may have access to or use of PHI.
- (3) Retraining. Existing workforce members must receive retraining no later than 45 days after there is material change in their job functions or in our DMH Privacy Policies and Procedures that affects their access to or use of PHI.

6d. Training Documentation. Your Privacy Officer or training officer will document completion of training of each workforce member on our DMH Privacy Policies and Procedures, using a privacy training certificate. The DMH Privacy Officers or training officers will send a copy of the completed certificates to the DMH Division of Human Resources for inclusion in the personnel file of the DMH workforce member trained.

6e. *Assurance of Confidentiality.* Each DMH workforce member shall be provided and shall sign FORM 15, Assurance of Preservation of the Confidentiality and Security of Protected Health Information, after role-based training has been completed on these policies and procedures. This form shall be placed in the workforce member's personnel record. Other Network participants are encouraged to use this form or a similar process.

7. **Workforce Sanctions.** DMH workforce members who violate our DMH Privacy Policies and Procedures, the HIPAA Privacy Rules or the DC Mental Health Information Act (MHIA) or other applicable federal or state privacy law shall be subject to discipline in accordance with Chapter 16 of the DPM and applicable collective bargaining agreements.

In addition to the workplace sanctions, consumers can seek civil and criminal penalties for violation of the MHIA, and may file a complaint with the U.S. Department of Health and Human Services for violation of HIPAA.

8. **Reporting Workforce Privacy Violations.** Each member of our workforce is obligated to report promptly any suspected violation of our DMH Privacy Policies and Procedures, the HIPAA Privacy Rules, MHIA, or other applicable federal or state privacy law to their Privacy Officer or designee. Reports may be made anonymously. Each workforce member must cooperate fully with any investigation, corrective action or sanction instituted by their Privacy Officer.

9. **Mitigation.** Network participants shall initiate corrective action whenever an improper use or disclosure of PHI occurs by one of their workforce members or business associates.

10. **Retaliatory Acts.**

10a. Network participants shall not tolerate any workforce member who attempts to intimidate, threaten, coerce, discriminate or retaliate against an individual who:

- Exercises any right, including filing complaints, under the DMH Privacy Policies and Procedures or other privacy laws.
- Complains to, testifies for, assists or participates in an investigation, compliance review, proceeding or hearing by the Department of Health and Human Services (HHS) or other appropriate authority.
- Opposes any act or practice the individual believes in good faith is illegal under the Privacy Rule (provided the opposition is reasonable and does not involve illegal disclosure of PHI).

10b. A workforce member who suspects that another workforce member has violated the ban on retaliatory acts must report the suspicion to their Privacy Officer or designee. Reports may be made anonymously. Each workforce member must cooperate fully with any investigation, corrective action or sanction instituted by their Privacy Officer.

11. **Document and Record Retention.** The DMH, DC CSA, and SEH Privacy Officers, must ensure that all documentation required by our DMH Privacy Policies and Procedures and the HIPAA Privacy Rules are maintained at least six (6) years after the later of its creation or last effective date. Other Network providers must retain their documentation in compliance with HIPAA. Each Privacy Officer or designee will ensure the following information is maintained in written or electronic form:

- The DMH Privacy Policies and Procedures and each revision of them.
- The DMH Privacy Practices Notices, each revision of them, and all documentation relating to our distribution of them.

- Each authorization and authorization revocation.
- Each request from consumers for access, amendment, disclosure accounting, restriction, or confidential communication, and all other documentation relating to our compliance with our obligations with respect to consumers' rights.
- Each complaint and any material generated as a result of investigating and resolving the complaint.
- Documentation evidencing designation of each Privacy Officer and any delegation of duties and responsibilities to the Privacy Officer's designees, designation of personnel and record sets, and designations with respect to covered entity structures.
- Documentation relating to personal representative relationships, business associate relationships, group health plan and plan sponsor relationships, limited data sets, and de-identified health information.
- Documentation of workforce training and sanctions, mitigation plans, and other administrative requirements.
- Other documentation requested or required under our DMH Privacy Policies and Procedures or demonstrating our compliance with our obligations under the HIPAA Privacy Rules.

12. **Data Privacy Protection.** DMH and all Network providers shall implement and comply with reasonable and appropriate administrative, physical, and technical safeguards to secure the privacy of PHI against any intentional or unintentional use or disclosure in violation of the Privacy Policies and Procedures or the HIPAA Privacy Rules. (Also see Part VII for security policies and procedures).

13. **Distribution/Location of the Manual.** The DMH Privacy Policies and Procedures Operations Manual shall be disseminated throughout the Department and made available to Network providers. DMH and each Network provider shall ensure that a copy of the manual is provided to all of their programs that require its use. It shall be placed in a prominent location where it is accessible to all employees that use and/or disclose PHI.

Approved By:

Martha B. Knisley  
Director, DMH

(Signature)

(Date)

## **TABLE OF CONTENTS**

### **DMH Policy 645.1, DMH Privacy Policies and Procedures**

- I. Use and Disclosure Policies and Procedures**
  - 1. Fundamental Policies on Use and Disclosure of Protected Health Information
  - 2. Authorization for Use or Disclosure
  - 3. Disclosures That Do not Require Written Authorization
- II. Standard Procedures**
  - 4. Minimum Necessary Determination
  - 5. Identity and Authority Verification  
(For standard Disclosure Log requirements, see Section 9, Disclosure Accounting)
- III. Consumers' Information Rights**
  - 6. Joint Notice of Privacy Practices
  - 7. Access
  - 8. Amendment
  - 9. Disclosure Accounting
  - 10. Restriction Requests
  - 11. Confidential Communication
- IV. Relationship Policies and Procedures**
  - 12. Authorization by Minors and Personal Representatives
  - 13. Business Associates
- V. Other Types of Disclosures**
  - 14a. Limited Data Set and Data Use Agreement
  - 14b. De-Identified Health Information
  - 15. Research - **RESERVED**
- VI. Consumer Complaints**
  - 16. Complaints and HHS Enforcement
- VII. SECURITY POLICIES AND PROCEDURES**
  - Fax Policy
  - Computer Security
  - Portable Devices Policy
  - Protection and Physical Security of PHI and DMH Sensitive Information
  - Antivirus and Malicious Code Software and Other Requirements
  - DMH Network Security

\*\*\*\*\*

**JUL 1 6 2003**

## **VIII. Definitions**

## **IX. Appendix**

**A – Schedule of Fees - RESERVED**

**B – Minimum Necessary Determination Checklist**

**C – Standard Agency Protocols for Routine or Recurring Disclosures - RESERVED**

**D – DMH-HIPAA Forms/Letters**

Form 1 – Joint Notice of Privacy Practices

Form 2 – Consent

Form 3 - Authorization

Form 4 – Identity and Authority Verification

Form 5 – Reserved

Form 6 – Disclosure Log

Form 7 – Access Request Form

Form 8 – Designated Personnel and Record Sets

Form 9 – Amendment Request

Form 10 – Request for Accounting

Form 11 – Restriction Request/Termination

Form 12 – Confidential Communication Request

Form 13 – Data Use Agreement

Form 14 – Complaint Form

Form 15 – Assurance of Preservation of the Confidentiality and Security of Protected Health Information

**E – Special Contract Requirements: Privacy Compliance Clause**

**F – Department of Mental Health Designated Record Sets Tool**

**JUL 16 2003**

## **I. USE AND DISCLOSURE POLICIES AND PROCEDURES**

### **1. Fundamental Policies on Use and Disclosure of Protected Health Information (PHI).**

Within the DC Mental Health Network, participating providers will maintain a Joint Notice of Privacy Practices, FORM 1, to give consumers written notice of the uses and disclosures of protected health information (PHI) within the Network. The Notice will be provided upon first service encounter with the consumer. Consumers will then be asked to sign a joint Consent, FORM 2, authorizing use and disclosure of PHI to participants in the Network. Copies of each will be given to the consumer and filed in the consumer's clinical record (See Section 6 of this manual regarding the Notice).

The DC Mental Health *Network* means an organized health care arrangement consisting of the Department of Mental Health (DMH), and every mental health provider that is certified, licensed, or otherwise regulated by DMH, or has entered into a contract or agreement with DMH for the provision of mental health services or mental health supports.

#### **1a) Treatment, Payment, Health Care Operations Within the DC Mental Health Network.**

Network participants may use and disclose PHI within the Network for the purposes of treatment, payment, and healthcare operations, but only to the minimum extent necessary, and only if the consumer has authorized such use and disclosure by executing a joint Consent, FORM 2. The DMH Privacy Officer or designee shall maintain and disseminate to designated staff a current list of Network Providers.

##### **Procedure.**

- (1) Before making any disclosure within the Network, you must confirm that:
  - The intended recipient of the PHI is a participating provider in the Network, and
  - The PHI to be disclosed is for treatment, payment, or health care operations of the Network, and
  - The consumer signed the joint Consent form.
- (2) If the consumer did not sign the joint Consent, disclosures may be made only pursuant to written authorizations signed by the consumer or the consumer's personal representative (See Section 2), except for disclosures that do not require written authorizations addressed in Section 3.

#### **1b) Treatment, Payment, Health Care Operations Outside the DC Mental Health Network.**

Network participants may use and disclose PHI outside the Network only if (1) the consumer has executed a written authorization specific to the intended use or disclosure or (2) one of the conditions described in Section 3 applies.

**Procedure.** Obtain authorization from the consumer in accordance with Section 2, if none of the Section 3 exceptions apply. **Use Form 4-Identity and Authority Verification**, to verify recipient (See Section 5).

- 1c) Within or outside the Network, employees may disclose PHI to other employees within the same mental health facility** to the minimum extent necessary to facilitate the delivery of mental health services to the consumer (includes treatment, payment, and healthcare operations).

*Mental health facility* means any hospital, clinic, office, nursing home, infirmary, or similar entity where professional services are provided; and any entity that is licensed or certified by, or has entered into an agreement with, DMH to provide mental health services or supports.

**1d) Consumer or Personal Representative.**

PHI may be disclosed to the consumer who is the subject of the PHI and to that consumer's personal representative as relevant to the scope of the request without written authorization. (See Section 12-Authorization by Minors and Personal Representatives for information about personal representative determination and status). The minimum necessary requirement does not apply to consumers and their personal representatives.

**Procedure.** Use Form 4 Identity and Authority Verification, to identify a consumer and/or a personal representative and their authority (See Section 5).

See also Section 7 of this manual on the consumer's right to inspect and copy his or her own PHI.

**1e) Incidental Use and Disclosure.**

Incidental use and disclosure of PHI *is not* permitted. Employ common sense and good judgment when using or disclosing PHI in conversation, by mail, electronic transmission or any other means, and when recording and storing PHI in any medium, to avoid any incidental use or disclosure of the PHI in connection with an otherwise permitted or required use or disclosure.

Examples of incidental use and disclosure include phone conversations related to PHI being inadvertently overheard, faxes being sent to incorrect fax numbers, faxes being sent to areas that are not secure, etc.

**Procedure.** If an incidental use or disclosure occurs, notify your supervisor and document the event on Form 6, Disclosure Log. If possible, notify the recipient that there has been an inadvertent disclosure and, if applicable, take actions to have the PHI returned or destroyed. If a pattern of such incidental use/disclosure becomes evident, disciplinary action may result.

## 2. Authorization for Use or Disclosure.

### 2a) Authorization

Network participants shall use Form 3, Authorization, for required written authorizations not covered by the joint Consent (except for disclosures that do not require written authorization addressed in Section 3 and for the conditioned authorization discussed in subsection 2c below).

Any consumer 18 years of age or over has the power to authorize use or disclosure of PHI. (See Section 12 on authorization by minors and personal representatives.)

#### Procedure.

(1) **Obtaining Authorization.** Your Privacy Officer or designee must approve your use or disclosure of a consumer's PHI pursuant to an authorization.

Whenever you seek, or a consumer directs, use or disclosure of his/her PHI for which authorization is required, you must:

- Provide Form 3, Authorization, to the consumer.
- Fill in, or have the consumer (or the consumer's personal representative) completely fill in, the authorization form.
- Have the consumer (or the consumer's personal representative) read, sign, and date the completed authorization form. An authorization that is incomplete, that you know contains false information, or that is not signed and dated is invalid. If the authorization form is signed by the consumer's personal representative, be sure that it shows the personal representative's name and the relationship that gives the personal representative authority to act on the consumer's behalf (Also see Section 12 on authorization by minors and personal representatives).
- Give the consumer (or the consumer's personal representative) a copy of the signed authorization form and provide the original to the Privacy Officer or designee for approval. Once approved, comply strictly with the terms of the authorization on use and disclosure of the PHI; if disapproved, follow the directions of the Privacy Officer or designee.

(2) **Authorizations Received From Third Parties.** If you receive an authorization from someone other than the consumer or the consumer's personal representative, take the actions below:

- Review Form 3, Authorization, to ensure it is complete, contains no false information, and is signed and dated by the consumer or consumer's personal representative.
- If the authorization form is signed by the consumer's personal representative, be sure that it shows the personal representative's name and the relationship that gives the personal representative authority to act on the consumer's behalf.
- Provide the original to the Privacy Officer or designee for approval prior to release of the PHI.

- Once approved, comply strictly with the terms of the authorization on use and disclosure of the PHI; if disapproved, follow the directions of the Privacy Officer or designee.

The original signed authorization must be filed in the consumer's clinical record, and a copy must be sent with the information to be disclosed.

(3) See subsection 2d below on revocation or expiration of the authorization.

(4) **Use FORM 4-Identity and Authority Verification**, to document how you verify the identity and authority of a person (consumer or personal representative) giving authorization; and to verify the identity of a third party presenting an authorization as one that the authorization allows to receive and use the PHI before you disclose it (see Section 5).

(5) **Minimum Necessary.** You are not required to limit the PHI used or disclosed to the minimum necessary, though you are confined to using and disclosing only the PHI identified by the authorization (See Section 4).

## **2b) Psychotherapy Process Notes and Information Received in Confidence.**

Psychotherapy process notes and notes regarding information received in confidence shall not be kept as part of the consumer's clinical record, but shall be maintained, if at all, by the mental health professional who created the notes.

(1) ***Psychotherapy Process Notes*** are notes made by a mental health professional documenting or analyzing the contents of conversations during an individual, joint, group, or family therapy or counseling session and maintained in a location separate from the consumer's clinical record. They typically contain intimate personal information, details of fantasies or dreams, process interactions, sensitive information about significant persons in the consumer's life, or the therapist's formulations and speculations.

Example: "Ms. Jackson reported several dreams during our session today. I suspect she is making up dreams to gain my approval as she knows I am a specialist in this area. Will monitor for further themes of need for approval by others in her life."

**Psychotherapy process notes are notes that are created by the treating mental health professional for his or her own use only and do not contain information typically needed by other members of the treatment team.**

Information needed by other members of the treatment team or for processing claims would not be considered psychotherapy process notes and would be kept as part of the consumer's clinical record. For example, notes pertaining to the following would not be psychotherapy process notes: medication prescription and monitoring; counseling session start and stop times; modalities and frequencies of treatment furnished; results of clinical tests and any summary of the following items: diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date.

Example: "Met with Ms. Jackson for a 30 minute counseling session today. She reports increased energy and has not missed any work this week. Overall she has shown improvement during the last month though she continues to have periods of high anxiety. Continue weekly sessions, renew current medications for 30 days. Consider changing anti-depressant to one with more anti-anxiety effects."

(2) ***Information Received in Confidence*** is information received from other persons on condition that such information not be disclosed to the consumer or other persons.

Example: Jerry Wilson's father called today asking to speak with this writer in confidence. He reported that his 14-year-old son was told his mother died from an accident to hide the fact of her suicide. Mr. Wilson fears his son's depression would be exacerbated if he knew this information.

Like psychotherapy process notes, notes regarding information received in confidence shall be kept only by the mental health professional, if at all.

**Procedure.**

No one can have access to psychotherapy process notes or notes regarding information received in confidence except in the following two instances: (1) the mental health professional may disclose them as needed if the consumer sues the mental health professional for malpractice or wrongful disclosure, and (2) the mental health professional must grant the consumer or the consumer's personal representative access to information received in confidence if granting access would not be reasonably likely to reveal the source of the information received (also see Section 7b).

**2c) Conditioned Authorization for Research.**

Refer all questions and requests for use and disclosures of PHI related to research to your Privacy Officer or designee (also see Section 15-Research).

**2d) Authorization Revocation or Expiration**

We may not rely on an authorization we know has been revoked or has expired. The consumer has the option of stating that the authorization will remain in effect for any period of time up to sixty (60) days, except in cases where the consumer authorized the disclosure in order to get life or health insurance.

A consumer may also revoke authorization at any time. Revocation of an authorization does not affect actions we may have undertaken in reliance on the authorization before we learned of its revocation.

**Procedure.**

(1) Check the consumer's clinical record to confirm that an authorization has not expired or been revoked before you use or disclose PHI pursuant to the authorization.

(2) If a consumer (or the consumer's personal representative) who has given authorization indicates a desire to revoke it, document the revocation as follows:

- Have the consumer (or the consumer's personal representative) fill in the date and sign the revocation section on the original Authorization, Form 3.
- Give the consumer (or the personal representative) a copy.

- Refile the original Form 3, with the revocation section filled out, in the consumer's clinical record. **2.4**

(3) **Verification.** Use Form 4-Identity and Authority Verification, to verify the identity of the consumer (and the identity and authority of a personal representative) revoking authorization (See Section 5).

JUL 16 2003

### **3. Disclosures That Do Not Require Written Authorization.**

The circumstances under which protected health information (PHI) may be used or disclosed without authorization for public health, public interest, public benefit, and law enforcement activities are very narrow, specific circumstances are described in the subsections below. In addition, disclosures to Health and Human Services (HHS) for complaint investigation or compliance enforcement or review do not require written authorization (See subsection 3h below).

#### **Procedure.**

- (1) Except in emergency situations that meet the description in subsections 3a, 3b(1) and 3b(3), consult your Privacy Officer or designee before disclosing PHI in response to any request, demand or legal process to use or disclose PHI that is not accompanied by the written authorization of the consumer or the consumer's personal representative.
- (2) **Verification.** Use **Form 4 - Identity and Authority Verification**, to verify the identity and authority of the person seeking use or disclosure of PHI in all of the circumstances described in this Section (See Section 5-Identity and Authority Verification).
- (3) Use **Form 6 - Disclosure Log**, to log each disclosure outlined in this Section **except** for disclosures to law enforcement officials when required by law. (See Section 9 for guidance on disclosure accounting.)
- (4) **Minimum Necessary.** Determine the minimum necessary PHI (see Section 4 of this manual) to use or disclose in all of the circumstances described in this Section except when required by law (subsection 3b) and for disclosures to Health and Human Services (subsection 3h).

### **Circumstances That Do Not Require Written Authorization:**

#### **3a) Public Health and Safety Threats.**

The minimum necessary PHI may be disclosed on an emergency basis to one or more of the following if a mental health professional reasonably believes that the disclosure is necessary to initiate emergency psychiatric hospitalization of the consumer pursuant to D.C. Code § 21-521 or to otherwise protect the consumer or another person from a substantial risk of imminent and serious physical injury.

- a consumer's spouse, parent, legal guardian,
- a duly accredited officer or agent of the District of Columbia in charge of public health,
- the Department of Mental Health,
- an individual or entity that is licensed or certified by, or has entered into an agreement with, DMH to provide mental health services or supports,
- an officer authorized to make arrests in the District of Columbia, or
- an intended victim.

JUL 16 2003

**3b) Required by Law.**

PHI may be disclosed to the extent required by law to meet the requirements of DC Official Code § 21-586 (concerning financial responsibility for the care of hospitalized persons) and to meet the compulsory reporting provisions of District or federal law that attempt to promote human health and safety. The following situations are examples of compulsory reporting laws:

(1) **Child Abuse:** If you are a physician, psychologist, medical examiner, dentist, chiropractor, registered nurse, licensed practical nurse, person involved in the care and treatment of consumers, law-enforcement officer, school official, teacher, social service worker, day care worker, or mental health professional, you are required by law to report or have a report made immediately if you know or have reasonable cause to suspect that a child known to you in your official capacity has been, or is in immediate danger of being, mentally or physically abused or neglected. If you believe you may have a duty to make such a report, you must immediately notify your supervisor and your Privacy Officer. This notification does not relieve you of your individual duty under the law to ensure that a report is made immediately to the Child and Family Services Agency's 24-hour reporting line at 202 671-SAFE (7233). Consult CMHS Policy 50000.630.2A, "Guidelines for the Evaluation and Reporting of Physical Abuse, Sexual Abuse, and Neglect of Children" for further guidance.

(2) **Child Fatalities:** The persons described in subsection 3b(1) above are also required by law to report to the Registrar of Vital Records as soon as practicable, but in any event within five (5) business days, the death of any child who is committed to the District's child welfare, mental retardation and developmental disabilities, or juvenile systems. We must also provide the Child Fatality Review Committee with immediate access to any and all records they request regarding a deceased child.

(3) **Adult Abuse:** The law also requires that social workers, licensed health professionals, and health care administrators immediately report to Adult Protective Services if, in their official capacity, they have substantial cause to believe that an adult is in need of protective services due to abuse or neglect by another. You must notify your supervisor or your Privacy Officer immediately as well.

**3c) Health Oversight Activities.**

The minimum necessary PHI may be disclosed to qualified personnel to carry out management audits, financial audits, quality improvement activities, or program evaluation of a mental health professional or mental health facility, provided that such personnel have demonstrated and provided assurances, in writing, of their ability to comply with all applicable federal and District privacy laws, including the requirement that they avoid revealing, directly or indirectly, the identity of any consumer whose information they receive. Prior to any disclosure being made, the Privacy Officer or designee will certify that assurances are adequate.

JUL 1 6 2003

**3d) Judicial and Administrative Proceedings.**

The minimum necessary PHI may be disclosed (1) by a mental health professional in order to initiate or seek civil commitment proceedings; and (2) in a civil or administrative proceeding in which the consumer, the consumer's representative, or in the case of a deceased person, any one claiming or defending through the consumer who makes the consumer's mental condition an element of the claim or defense.

In addition, PHI may be disclosed in response to a judicial or administrative order, provided we disclose only the expressly ordered information, and it may be disclosed in response to a subpoena or other process, but only if either the consumer has executed an authorization or a judge has authorized the disclosure in writing.

In litigation for the collection of fees, no PHI other than administrative information shall be disclosed, except to the extent necessary (1) to respond to a motion of the consumer or the consumer's representative for greater specificity; or (2) to dispute a defense or counterclaim. ("Administrative information" consists of the consumer's name, age, sex, address, identifying number or numbers, dates and character of sessions [individual or group], and fees.)

Refer any request for court related disclosures to the Privacy Officer or designee.

**3e) Law Enforcement.**

Unless one of the exceptions described in this Section applies, PHI may not be disclosed to a law enforcement officer without the consumer's written authorization.

**3f) Research.** For authorizations related to research refer to Section 15.**3g) Protection and Advocacy Organization ("ULS").** We are required by federal law to grant access in most instances to records requested by the designated organization responsible for protection and advocacy ("P&A") in the District of Columbia for persons with mental illness (currently University Legal Services, or "ULS"). ULS is authorized to investigate allegations of abuse and neglect and pursue legal remedies on behalf of individual consumers. In certain narrow circumstances, ULS is entitled to have access to a consumer's records even if they do not have written authorization from the consumer or the consumer's personal representative. If you receive a request for disclosure of protected health information from a representative of ULS, or any other organization representing itself as the P&A organization, and the requestor does not present an authorization signed by the consumer or the consumer's personal representative in accordance with Sections 2 and 12, consult your Privacy Officer before disclosing or granting access to the protected information.**3h) Required Disclosures to Health and Human Services (HHS).**

PHI must be disclosed to HHS as required for complaint investigation or compliance enforcement or review.

**Procedure.**

(1) Promptly notify your Privacy Officer or designee upon receipt of a request for PHI from HHS. Do not disclose any PHI in response to an HHS request unless and until you receive instruction from your Privacy Officer or designee. Your Privacy Officer or designee will coordinate your responses to HHS requests.

(2) **Disclosure Log.** Use Form 6-Disclosure Log, to document disclosure.

(3) **Minimum Necessary.** You are not required to limit to the minimum necessary.

JUL 16 2003

## II. STANDARD PROCEDURES

### 4. Minimum Necessary Determination

#### 4a) Workforce Use.

As a member of our workforce, you will access and use only the minimum necessary protected health information (PHI) reasonably needed to perform your duties for the Network. You must not attempt to access or use more than the minimum necessary PHI needed to perform your duties. If you have questions consult your Privacy Officer or designee.

Always use and disclose only the minimum necessary PHI except where it is not applicable as stated below.

#### Minimum Necessary Not Applicable When:

- The recipient of the requested PHI is either the consumer who is the subject of the information or the consumer's personal representative.
- The consumer or the consumer's personal representative authorized the disclosure pursuant to Section 2.
- The disclosure is required by the Department of Health and Human Services (HHS) for complaint investigation or compliance enforcement or review.
- The disclosure is required by law.
- The disclosure is required for compliance with the HIPAA Administrative Simplification Rules.
- The disclosure involves de-identified information.

#### Procedure.

(1) Routine or Recurring Disclosures and Requests. Follow the standard protocols applicable to a particular routine or recurring disclosure of or request for PHI. Your Privacy Officer or designee will issue standard protocols for the minimum necessary PHI for specified routine or recurring disclosures and requests. (See Appendix C at the back of this manual).

(2) Non-Routine and Non-Recurring Disclosures or Requests. Do not disclose or request PHI for a non-routine and non-recurring purpose until you review the situation on an individual basis against our standard criteria to ensure that only the minimum necessary PHI for the purpose is disclosed or requested. Refer to Section D of the minimum necessary checklist in Appendix B at the back of this manual. If you question whether a particular disclosure or request should be subject to an individual review (rather than treated as routine or recurring) or how to conduct the individual review based on our criteria, consult your Privacy Officer or designee.

**4b) Entire Clinical Record.** When an entire clinical record is to be used, disclosed or requested, you must:

- Determine on an individual basis whether the situation justifies using, disclosing or requesting an entire clinical record as the minimum necessary PHI for the purpose.
- Whenever the entire clinical record is requested by individuals outside the Network, the Privacy Officer must approve the release of the entire record.

*(The entire clinical record constitutes all documentation in the clinical record(s) on a consumer.)*

## **5. Identity and Authority Verification.**

You must verify the identity and authority of any person or entity who is requesting or authorizing disclosure of protected health information (PHI) before you disclose PHI. Use **FORM 4—Identity and Authority Verification**, to document the verification.

### **Procedure.**

(1) **Verification of Identity and Authority.** Obtain appropriate identification and, if the person is not the consumer who is the subject of the PHI sought, evidence of authority. If you question whether you have obtained sufficient verification, consult your Privacy Officer or designee before you make any disclosure.

a) **Evidence of Identification.** Examples of appropriate identification include:

- Photographic identification card.
- Government identification card or badge.
- Appropriate document on government letterhead.

If a person purports to be acting on behalf of a public official, appropriate identification includes, if reasonable for the situation:

- A written statement of appointment on appropriate government letterhead.
- A contract, memorandum of understanding, purchase order or other evidence establishing the appointment to act on behalf of the public official.

(b) **Evidence of Authority.** Examples of appropriate authority include, if reasonable for the situation:

- Identification as parent, guardian, or other person authorized by a court or by law to act for a minor; executor or administrator with respect to a deceased consumer or an estate; power of attorney or other evidence of legal authority to act on behalf of a consumer with respect to health care; or other evidence of appropriate relationship with the consumer with respect to health care.
- A warrant, subpoena, or other legal process bearing an indication that the court has approved the disclosure; or an order issued by a court, or an administrative tribunal.
- A written statement of legal authority or, with respect to a properly identified government official, an oral statement of authority, if reliance on such oral statement is reasonable for the situation. You must document the oral statement on FORM 4.

(2) **Documentation.** The completed FORM 4 must be filed in the consumer's clinical record.

### III. CONSUMERS' INFORMATION RIGHTS

#### 6. Joint Notice of Privacy Practices.

Within the DC Mental Health Network, participating providers will maintain a Joint Notice of Privacy Practices, FORM 1, to give consumers written notice of the uses and disclosures of protected health information (PHI) that the Network may make, and of the consumers' rights and the Network's legal duties with respect to PHI. The Network will always use and disclose PHI consistent with our Notice. We will furnish our Notice to any person who requests one.

Only the Joint Notice of Privacy Practices that has been approved by the DMH Privacy Officer may be distributed to Network providers. The DMH Privacy Officer will ensure the Notice and any revisions to it are consistent with DMH policy, District policy, the HIPAA Privacy Rules, and any other applicable local and federal laws.

The Network providers may use the Joint Notice of Privacy Practices as long as each agrees to be bound by the Notice's terms with respect to all PHI created or received pursuant to participation in the Network.

#### Procedure.

(1) Distribution of the Network's Joint Notice of Privacy Practices. The Department of Mental Health (DMH) will ensure that the Notice is electronically available on each web site we maintain that provides information about our services. Participating Network providers will disseminate the Joint Notice of Privacy Practices to each consumer by:

- Furnishing the Notice upon first contact:
  - Furnish the Notice by personal delivery if the first service delivery is a consumer visit.
  - Deliver the Notice by an electronic response if the first service delivery is by electronic mail.
  - Promptly mail the Notice if the first service delivery from the provider is by telephone.
  - Disseminate the Notice to each new consumer at enrollment.
- Posting the Notice in a clear and prominent place at each of the service delivery sites so that consumers seeking service may reasonably be expected to be able to read the Notice.
- In an emergency treatment situation, furnishing the Notice as soon as reasonably practicable after the emergency has abated.
- Disseminating the revised Notice, resulting from any material change that is adopted in the Network's privacy practices. Network participants must not implement any material change in the privacy practices before the effective date of the revised Notice (unless earlier implementation is required by law).

Network providers will notify consumers that the terms of the Notice have been changed by posting it at service delivery sites, and DMH will tell people who call the Access Help Line at 1-888-793-4357 or 202-561-7000. DMH will also post the changed Notice on the Internet at <http://www.dmh.dc.gov>

JUL 16 2003

The Notice may be emailed to any consumer who has agreed to electronic notification and not withdrawn that agreement. A paper copy of the Notice must be provided to the consumer, if you know the consumer failed to get the email transmission of the Notice or if the consumer requests a paper copy.

(2) **Acknowledgment for the Joint Notice of Privacy Practices.** To indicate receipt, we will require the consumer's signature on the acknowledgement of receipt page of the Notice. The acknowledgement of receipt page of the Notice shall be filed in the consumer's clinical record.

We will make a good faith effort to obtain a consumer's signature at the first service encounter. If the consumer fails or refuses to sign the Notice we will document our effort to obtain it on the acknowledgement of receipt page of the Notice and file it in the consumer's clinical record.

If our first service encounter is an emergency treatment situation, we do not need to seek signature on the Notice from the consumer at that time, however the consumer's signature should be obtained as soon thereafter as possible.

Consumers who do not write can be directed to sign using an X with a witness to verify and note they observed this activity by the consumer. For consumers who do not read, the Notice can be read to them.

## 7. Access.

### 7a) Right to Inspect and Copy.

- (1) We will respond to all requests for access to protected health information (PHI) within thirty (30) days of receipt of the written request, including providing the requesting party either with photocopies or the opportunity to inspect and photocopy the requested information as long as we or our business associates maintain it in designated record sets (See subsection 7d below on designated record sets).
- (2) A mental health professional, responsible for the diagnosis or treatment of the consumer, shall have the opportunity to discuss the PHI with the consumer at the time of such inspection.
- (3) In the case of a request for access directed to a data collector, the data collector may grant access either directly to the requestor or indirectly by providing the requested information to a mental health professional designated by the requestor.
- (4) If the mental health professional designated by the requestor is not the person who disclosed the information to the data collector, he or she shall be in substantially the same or greater professional class as the professional who disclosed the information to the data collector.

*Data collector* means a person, other than the consumer, mental health professional and mental health facility who regularly engages, in whole or in part, in the practice of assembling or evaluating consumer protected health information.

### Procedure.

- (1) **Access Request.** Since we must take action on the request within thirty (30) days of receipt, do not delay transmitting an access request to your Privacy Officer or designee. Complete, or have the consumer complete, the first page of FORM 7–Access Request, then promptly transmit the entire FORM 7 to your Privacy Officer or designee by the next business day.
- (2) **Access Fees.** We may charge a reasonable, cost-based fee for copying and mailing of the requested PHI, and for preparing a summary or explanation of the requested PHI. We may not charge for providing access to or retrieving the requested PHI. Your Privacy Officer or designee will determine any charges and inform the consumer in advance so that the consumer may elect to withdraw or modify the request to reduce or avoid the fee. See the schedule of fees in Appendix A at the back of this manual. Access fees will not apply to indigent (unable to pay) consumers. Consult with your financial officer or other responsible person identified by your agency if there are questions regarding determination of indigence.
- (3) **Access Response.** Based on the recommendation of a mental health professional whether to grant or deny a consumer access to PHI, your Privacy Officer or designee will process each access request as follows:
  - Coordinate and track the processing of the access request on page 2 of Form 7,

- Inform the consumer whether access is granted or denied in writing (with a statement of the reasons for denial, and the procedures for complaining to us and to Department of Health and Human Services about a denial), and
- If access is granted, inform the consumer of any applicable fees to ensure that the consumer still wants access, copies, a summary or explanation, or mailing.
- Notify affected business associates in writing to retrieve records.
- Have the completed FORM 7 and notification letters included in the consumer's clinical record.

(4) **Access Granted.** We will permit a consumer who has been granted access the opportunity to inspect and obtain a copy of his or her PHI at a time and place, or by mail, as may be mutually agreed by the consumer and your Privacy Officer or designee. We will provide the consumer a summary or explanation of the requested PHI, if the consumer requests and agrees to pay any fee we may charge for preparing the summary or explanation.

If instructed by your Privacy Officer or designee to supervise a grant of access, you will furnish the requested PHI in the form or format that the consumer requests, unless that is not feasible. Consult with the Privacy Officer or designee if it appears that the form or format the consumer requests is not feasible. If your Privacy Officer or designee informs you that there is a fee, you must collect the fee before providing the access service to which the fee applies.

#### **7b) Protected Health Information We May Withhold.**

(1) **Denial of Access without Right of Review.** A mental health professional may deny access to information received in confidence if granting the access requested would be reasonably likely to reveal the source of the information (see Section 2b of this manual).

(2) **Denial of Copies to Inmates.** We may not withhold access to PHI from inmates of correctional facilities unless the criteria in subsection (3) below are satisfied.

(3) **Denial of Access to Dangerous Information.** A mental health professional or mental health facility may limit the disclosure of portions of a consumer's record of PHI to the consumer only if:

- the mental health professional primarily responsible for the diagnosis or treatment of such consumer reasonably believes that such limitation is necessary to protect the consumer from a substantial risk of imminent psychological impairment; or
- to protect the consumer or another person from a substantial risk of imminent and serious physical injury. The mental health professional shall notify the Privacy Officer or designee and the consumer will be notified in writing of any denial of access, whether the denial is in whole or in part.

(4) When PHI access is denied, your Privacy Officer or designee will:

- (a) Inform the consumer of the denial in writing and of the right of independent review and the procedures for exercising that right.

- (b) The consumer may designate an independent mental health professional who shall be permitted to review the consumer's record of PHI as a result of our denial of access on grounds of endangerment within a reasonable time and report to the Privacy Officer or designee whether the denial is justified.

**7c) Review of Access Denial for Endangerment.**

The independent mental health professional shall be in substantially the same or greater professional class as the mental health professional who initially recommended the limited disclosure.

- (1) The independent mental health professional shall permit the consumer to inspect and duplicate those portions of the consumer's record of PHI which, in his or her judgment, do not pose a substantial risk of imminent psychological impairment to the consumer or pose a substantial risk of imminent and serious physical injury to the consumer or another person.

In the event that the independent mental health professional allows the consumer to inspect and duplicate additional portions of the consumer's record of PHI, the mental health professional primarily responsible for the diagnosis or treatment of the consumer shall have the opportunity to discuss the information with the consumer at the time of transmittal, examination or duplication of information.

- (2) The consumer may bring a lawsuit in the Superior Court within six (6) months of being denied access if the independent mental health professional denies access in whole or in part, or if the consumer is indigent and is unable to obtain the services of an independent mental health professional. In such a lawsuit, the mental health professional will have the burden of proving by a preponderance of the evidence that the denial of access was appropriate.

**7d) Identification of Designated Record Sets.**

We must identify in writing each designated record set we maintain or that is maintained on our behalf by our business associates, and the titles of persons or offices responsible for receiving and processing access requests. (See Appendix F for the DMH designated record sets tool.)

*Designated Record Set* means a group of records maintained by or for DMH, other Network providers, and business associates that is: the medical and billing records relating to a consumer maintained by or for a health care provider; the enrollment, payment, claims adjudication, and case or medical management systems maintained by or for a health plan, or; used, in whole or part, by or for a covered entity to make decisions about consumers.

Each Privacy Officer or designee must document on FORM 8-Designated Personnel and Record Sets the persons or job categories responsible for receiving and processing access requests in the agency, and the designated record sets maintained by the agency or for the agencies by business associates. Send the completed FORM 8 to the DMH Privacy Officer or designee and maintain a copy in the Privacy Officer file. Promptly update FORM 8 upon any change in designated personnel or record sets.

## **8. Amendment.**

### **8a) Right to Amend.**

A consumer may request to amend his or her PHI for as long as we or our business associates maintain the PHI in designated record sets. We may deny an amendment request only as specified in subsection 8b below.

#### **Procedure.**

(1) **Amendment Requests.** We are obligated to respond to the consumer's request to amend within sixty (60) days of its receipt. Consequently, transmit the amendment request to your Privacy Officer or designee by the next business day.

Complete, or have the consumer complete, the first page of FORM 9–Amendment Request, then promptly transmit the entire FORM 9 to your Privacy Officer or designee.

(2) **Amendment Response.** The Privacy Officer will coordinate with the mental health professional as required. Based on the recommendation of the responsible mental health professional to grant or deny a consumer's amendment request, your Privacy Officer or designee will process each amendment request as follows:

- Coordinate and track the processing of the amendment request on FORM 9.
- Respond in writing to a consumer's request to amend within sixty (60) days. (The initial response may be written notice that a thirty (30) day extension of the sixty (60) day response period will be taken for reasons stated in the notice including the date that we will provide our response.) Inform the consumer in writing whether the amendment will be granted or denied.
- If amendment is granted, inform the organization head or designee, and business associates with affected designated record sets (in writing) that they are required to amend the record. Furnish the amendatory material to append or link to the affected records so that thereafter each disclosure is only of the properly amended records.
- If amendment is denied, you must also inform heads of agencies and business associates with affected designated record sets (in writing), and furnish the required materials to append or link to the affected records so that they can be included with future disclosures of those records.
- Have the completed FORM 9 and notification letters included in the consumer's clinical record.
- Sample notification letters are attached to Form 8 at the back of this manual.

### **8b) Basis for Denying Amendment Request.**

We may decline to amend PHI if:

- We did not create the information (unless the consumer provides a reasonable basis to believe the originator is no longer available to act on the request).
- The information to be amended is not part of a designated record set maintained by us or by a business associate on our behalf.
- The information is accurate and complete.
- The information to be amended may be withheld from the right of access. See Section 7(b).

**8c) Amending on Another Covered Entity's Notice.**

We will amend PHI in our designated record sets upon receipt of notice from a covered entity that the PHI has been amended.

**Procedure.**

Promptly inform your Privacy Officer or designee upon receipt of a notice from a covered entity that PHI has been amended, and send the notice to your Privacy Officer or designee. The Privacy Officer or designee will:

- Determine if we hold the affected PHI in our designated record sets or in designated record sets held on our behalf by business associates, and
- Notify and instruct the heads of agencies and our business associates with affected designated record sets (in writing) to amend the affected records, so that thereafter each disclosure is only of the properly amended records.

## **9. Disclosure Accounting.**

### **9a) Right to Disclosure Accounting.**

Upon a consumer's request, we will provide an accounting of each disclosure that is made of the consumer's PHI for up to six (6) years prior to the request.

Essentially, we are obligated to account for disclosures we make without the consumer's authorization (See Section 3) unless they are exempt from accounting as described below, or that violate the HIPAA Privacy Rules.

We do not have to account for disclosures that are exempt from accounting as follows:

- Disclosures made before April 14, 2003.
- Disclosures made within the Network for treatment, payment, or health care operations.
- Disclosures made to the consumer or the consumer's personal representative.
- Disclosures made pursuant to authorization.
- Disclosures made as part of a limited data set.
- Disclosures of de-identified PHI.
- Disclosures to business associates.
- Disclosures that are for national security or intelligence purposes.
- Disclosures made to correctional institutions or other law enforcement officials having lawful custody over an individual.

### **Procedure.**

(1) We are obligated to respond to the consumer's request for a disclosure accounting within sixty (60) days of its receipt.

- Complete, or have the consumer complete, the first page of FORM 10–Disclosure Accounting Request.
- Promptly transmit the entire FORM 10 to your Privacy Officer or designee by the next business day.

(2) **Accounting Fees.** We may not charge for a consumer's first accounting in any 12 month period. We may charge a reasonable, cost-based fee for other accountings within that same 12-month period. Refer to the standard schedule of fees in Appendix A at the back of this manual.

(3) **Accounting Response.** Your Privacy Officer or designee will process a consumer's request for disclosure accounting as follows:

- Determine if there are fees for the consumer's accounting request. If there are, notify the consumer in advance of the fee so that the consumer may elect to withdraw or modify the accounting request to reduce or avoid the fee.

JUL 16 2003

- Coordinate and track the processing of the accounting request on page 2 of FORM 10. Direct our agencies and business associates in writing to furnish the disclosure data needed to comply with the accounting request.
- Respond in writing to the consumer's accounting request within sixty (60) days. (The initial response may be written notice that a thirty (30) day extension of the sixty (60) day response period will be taken for reasons stated in the notice including the date that we will provide our response.) Inform the consumer, in writing, that the disclosure accounting is available or to transmit the disclosure accounting to the consumer.
- Have the completed FORM 10 and notification letters filed in the consumer's clinical record.
- Sample notification letters are attached to Form 10 at the back of this manual.

**9b) Accounting Information.**

We will track and record, and require our business associates to track and record accountable disclosures, and make the tracking information available to the Privacy Officer or designee on request, so that we may fulfill our obligations to make disclosure accounting to consumers on request. If you question whether a particular disclosure needs to be recorded, consult your Privacy Officer or designee.

**Procedure.**

- (1) Use Form 6 – Disclosure Log, to document each accountable disclosure you make.
- (2) The completed Form 6 must be filed in the consumer's clinical record. A copy must be filed in the Privacy Officer or designee file, and maintained for at least six (6) years to support our disclosures.

**9c) Accounting Content for Disclosure.** The following information for each accountable disclosure of PHI (including disclosures to or by our business associates) must be recorded and maintained for at least six (6) years to support our disclosure accounting obligations.

- The disclosure date;
- The name and, if known, address of each person or entity that received the disclosure;
- A description of the PHI disclosed; and
- A statement of the purpose of the disclosure, or a copy of any written request for the disclosure from HHS or another government agency or organization to which the PHI was disclosed under one of the subsections in Section 3.

**9d) Accounting Content for Repetitive Disclosures.** For multiple disclosures for a single compliance review or complaint investigation, or to another government

agency or organization to which we disclosed PHI pursuant to a single provision in Section 3, we need provide the consumer only:

- The frequency, periodicity, or number of the repetitive disclosures during the accounting period; and
- The date of the last disclosure during the accounting period.

## **10. Restriction Requests.**

### **10a) Requests.**

- A consumer may request that we restrict our use or disclosure of his or her protected health information (PHI) for treatment, payment, health care operations, or with specified family members or others.
- We strongly support consumer choice unless it is clinically contraindicated as determined by the clinical team. We will comply, and notify our business associates to comply with any such agreement we make (except in a medical/psychiatric emergency).

#### **Procedure.**

##### **(1) Requests.**

If a consumer makes a request to restrict disclosure of his or her PHI, responsible clinical staff must follow all applicable procedures of CMHS Policy 50000.515.5, Consumer Statement of Treatment Preferences, and document and adhere to the consumer's restriction of information choices as required.

In addition, based on that request, *responsible staff* will complete the first page of FORM 11–Restriction Request, have the consumer sign it, then promptly transmit the entire FORM 11 to their Privacy Officer or designee by the next business day.

**(2) Response.** Based on the conclusion of the clinical team, your Privacy Officer or designee will process each restriction request as follows:

- Coordinate and track the processing of the restriction request on page 3 of FORM 11.
- Notify the consumer, in writing, that we agree to or we deny the restriction.
- If we agree to the restriction, notify affected agencies and business associates, in writing, of their obligation to comply with the restriction.
- Have the completed FORM 11 and the notification letters included in the consumer's clinical record.
- Sample notification letters are attached to FORM 11 at the back of this manual.

### **10b) Medical/Psychiatric Emergency Exception.**

Restricted PHI may be used or disclosed to a health care provider, if the information is needed in a medical/psychiatric emergency for treatment of the consumer who is the subject of our restriction agreement.

#### **Procedure.**

(1) When requested to disclose restricted PHI for treatment in a medical/psychiatric emergency you must:

- Exercise professional judgment to determine that a medical/psychiatric emergency exists that justifies using or disclosing the restricted PHI.

- Document the basis for your determination, whether it resulted in using, disclosing or withholding the restricted PHI.
  - Send your documentation to your Privacy Officer or designee, and include a copy in the consumer's clinical record.
- (2) If you disclose restricted PHI to a health care provider for treatment in a medical/psychiatric emergency you must:
- Ask the health care provider to not further use or disclose the restricted PHI.
  - Document your request, and send your documentation to your Privacy Officer or designee. Include a copy in the consumer's clinical record. Your Privacy Officer or designee will follow up with the health care provider to document our request that there will be no further use or disclosure of the restricted PHI.

#### **10c) Unenforceable Restrictions.**

We will neither agree to, nor comply with, a restriction request for disclosures that do not require written authorization (See Section 3).

##### **Procedure.**

- (1) If you receive a restriction request that is unenforceable, notify your Privacy Officer or designee who will inform the consumer in writing that the restriction agreement cannot prevent uses or disclosures.
- (2) You must promptly notify your Privacy Officer or designee if you receive a request for restricted PHI from HHS or another government agency or organization. Follow the direction of your Privacy Officer or designee regarding the response to such request.

#### **10d) Restriction Termination.**

Based on a consumer's request, we may terminate the restrictions for disclosure of PHI.

**Procedure.** If the consumer wants to terminate a restriction agreement, complete the Termination section on page 2 of FORM 11, and submit the entire form to your Privacy Officer or designee. The Privacy Officer or designee will do the following:

- Notify the consumer, in writing, that we are terminating the restriction agreement as requested.
- Inform the agency head, or designee, of affected agencies and business associates, in writing, of the termination of the restriction agreement.
- Have the completed FORM 11 and notification letters included in the consumer's clinical record.
- Sample notification letters are attached to Form 11 at the back of this manual.

**Responsible clinical staff.** As a result of a restriction termination, responsible clinical staff will follow CMHS Policy 515.5, and have consumer's preferences updated on the appropriate form and filed in the clinical record.

**11. Confidential Communication.**

A consumer may request confidential communications (that is, the use of alternative means or alternative locations when we communicate protected health information (PHI) to the consumer), if the request is reasonable and in writing.

**Procedure.****(1) Requests.**

- a. If you receive a consumer's request that we use alternative means or locations when communicating PHI to the consumer, complete or have the consumer complete the first page of FORM 12-Confidential Communication Request, then promptly transmit the entire FORM 12 to your Privacy Officer or designee by the next business day.
- b. Consult with your Privacy Officer or designee before making a communication of PHI, if there is any question whether that communication should be treated as a confidential communication.
- c. You are not allowed to require a consumer to explain the basis for requesting confidential communications, nor may you question the validity of the consumer's representation that confidential communication is needed because of danger to the consumer.

**(2) Response.** Only your Privacy Officer or designee may approve a request for confidential communication of PHI. Your Privacy Officer or designee will process each confidential communication request as follows:

- Coordinate and track the processing of the confidential communication request on Form 12.
- Respond to the consumer by means and location appropriate to the confidential communication request. Your Privacy Officer or designee will inform the consumer whether we will accommodate the confidential communication request or whether the request cannot be accommodated without additional information.
- If we accommodate the confidential communication request, notify affected agencies and business associates in writing of their obligation to comply with the confidential communication request.
- If the consumer's request does not contain all of the information requested on the form, inform the consumer that we will not accommodate the confidential communication request without additional, specified information. The response must use the means or location appropriate to the confidential communication request.
- Have the completed FORM 12 and notification letters (as applicable) included in the consumer's clinical record.
- Sample notification letters are attached to Form 12 at the back of this manual.

#### IV. RELATIONSHIP POLICIES and PROCEDURES

##### 12. Authorization by Minors and Personal Representatives.

###### 12a) Personal Representatives of Adults and Emancipated Minors.

For purposes of authorizing use of, disclosure of, or access to, protected health information (PHI), a personal representative may be a person specifically authorized by the consumer in writing, or by a court, as the legal representative of the consumer, or a person otherwise authorized by law to make health care decisions on behalf of the consumer.

*"Emancipated minors"* are minors who live apart from their parents or legal guardians and manage their own personal and financial affairs, regardless of whether their parents or legal guardian consent to the arrangement, regardless of the duration of the arrangement, and regardless of the source of the minor's income.

- (1) We may use and disclose to a personal representative of an adult or emancipated minor that PHI relevant to the scope of the representation.
- (2) We will furnish a personal representative the same access to and disclosure accounting for a consumer's PHI that must be accorded the consumer, provided the access or disclosure accounting involves PHI relevant to the scope of the representation.

**Procedure.** Consult your Privacy Officer or designee if there is any question regarding required disclosure to a personal representative of an adult or emancipated minor. See Section 7-Access and Section 9-Disclosure Accounting for information about consumer's rights to access and for disclosure accounting of PHI.

###### 12b) Personal Representatives of Unemancipated Minors.

For purposes of authorizing use of, disclosure of, or access to an unemancipated minor's PHI, a personal representative may include a parent, a legal guardian, a person specifically authorized by a court to act on behalf of the minor, or a person authorized by law to make health care decisions on behalf of the minor.

- (1) **General rule:** For minors under the age of 14, use, disclosure, or access may be authorized only by the personal representative. For minors at least age 14 but under age 18, use, disclosure, or access must be authorized by both the personal representative and the minor.
- (2) **Exception:** A minor may authorize use of, disclosure of, or access to his or her own PHI under the following circumstances:
  - (a) **Minor's Consent to Health Care.** The minor agrees to the health care, no other agreements are required by law (even if the agreement of others has been obtained), and the minor has not requested a parent, guardian, or other person to be regarded as a personal representative.
  - (b) **Minor's Lawful Receipt of Health Care.** The minor, a court, or a legally authorized person agrees to the health care, and the minor could lawfully obtain the health care without the consent of a parent, guardian, or other person with authority to consent.

(c) **Parental Consent to Confidentiality.** The parent, guardian, or other person with authority to act for the minor consents to a confidentiality agreement between the minor and the health care provider regarding the health care.

**Procedure.** Consult with your Privacy Officer or designee if there are any questions of any type related to access to and disclosure of an unemancipated minor's PHI. See Section 7-Access and Section 9- Disclosure Accounting for information about consumer's rights to access and for disclosure accounting of PHI.

#### **12c) Personal Representatives of Deceased Consumers.**

(1) **Information Protected.** We will accord the PHI of a deceased consumer all of the privacy protections of these DMH Privacy Policies and Procedures.

(2) **Rights of Executors.** We will furnish an executor, administrator or other person authorized by the consumer in writing, or by a court, to act for the deceased consumer or the deceased consumer's estate, the same rights with respect to the deceased consumer's PHI that must be accorded living consumers, provided the PHI is relevant to the scope of the representation.

**Procedure.** Consult your Privacy Officer or designee if there is any question regarding the right of an executor, administrator or other person authorized to act for a deceased consumer or the estate.

#### **12d) Abusive Personal Representative.**

We will not consider a person to be a personal representative, and will not disclose any PHI to that person, if we have a reasonable belief that:

- the person has subjected or may subject the consumer to abuse, neglect or domestic violence, and that acknowledging the representative could endanger the consumer; or
- in authorizing disclosure of, or requesting access to, the consumer's PHI, the representative is not acting in the consumer's best interest.

#### **Procedure. Abusive Personal Representative.**

- Document the reasons for your suspicions in the consumer's clinical record.
- Consult and follow instructions from your Privacy Officer or designee before you disclose a consumer's PHI to a personal representative you suspect may be abusive.
- See **Section 3b, Required by Law**, for information about reporting child and adult abusive relationships to appropriate government authority.

### **13. Business Associates.**

Business Associate (BA) means a person or entity who, on behalf of DMH, and other than in the capacity of a workforce member: performs or assists in the performance of a function or activity that involves the use or disclosure of protected health information (PHI), or; provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services which involves the disclosure of individually identifiable PHI from DMH, or from another business associate of DMH, to the person or entity.

#### **13a) Uses and Disclosures with Business Associates.**

Protected health information (PHI) may not be disclosed to a business associate, and a business associate may not be allowed to create or receive PHI on our behalf, unless the responsible Privacy Officer has agreed to the arrangement and the Privacy Compliance Clause (see Appendix E) is a part of the agreement with the business associate.

The DMH manager who has direct authority and control over the release of PHI shall inform the DMH Contracting Officer and their Privacy Officer, in writing, that they wish to contract with a business associate. The Privacy Officer will request any information needed for review; and if the Privacy Officer agrees with the proposed arrangement, the contracting process shall proceed. If the Privacy Officer does not agree with the arrangement, the Privacy Officer will promptly inform the manager and/or the DMH Contracting Officer to reach a resolution.

The DMH Contracting Officer is responsible for completing the contracting process and ensuring that any agreements that involve the use of PHI have the appropriate Privacy Compliance Clause included in the agreement.

#### **13b) Business Associate Compliance.**

If a Privacy Officer learns that a business associate has materially breached their agreement, the business associate will be required to promptly cure the breach. If the business associate fails to cure the breach to our satisfaction, we will terminate the agreement. If termination of the agreement is not feasible, we will report the breach to Department of Health and Human Services.

**Procedure.** Immediately notify and cooperate with your Privacy Officer if you learn that a business associate may have breached or violated their agreement. You must follow the instructions of your Privacy Officer regarding investigation and resolution of the suspected breach or violation.

#### **13c) Our Organization as Business Associate.**

(1) We may serve as the business associate of a covered entity (for example, we may provide billing services, practice management, provide administrative services only or third party administration for a group health plan, or electronic transaction translation and transmission as a health care clearinghouse for other health care providers). When we serve as a business associate of a covered entity, we will enter into a business associate agreement with that covered entity.

(2) We will fully comply with the terms of each agreement we enter into as a business associate of a covered entity.

**Procedure.**

(1) You must obtain the approval of your Privacy Officer for any business associate agreement you may be asked to accept on behalf of our organization before you may undertake any business associate function or activity involving PHI.

(2) You must immediately notify and cooperate with your Privacy Officer if you learn that we may have breached or violated our business associate agreement with a covered entity. You must follow the instructions of your Privacy Officer regarding investigation and resolution of the suspected breach or violation. Our failure to comply with our business associate agreement obligations can expose our organization to sanctions under the HIPAA Privacy Rules.

**13d Documentation.**

The Privacy Officer will maintain a list of organizations and persons with which DMH has a business associate agreement. The Privacy Officer will also retain all documentation we create or receive regarding compliance of our business associates or our compliance as a business associate of covered entities, until six (6) years after the later of their creation or last effective date.

JUL 16 2003

## V. OTHER TYPES OF DISCLOSURES

### 14a) Limited Data Set and Data Use Agreement.

Network participants are permitted to use and disclose protected health information (PHI) included in a limited data set without obtaining an Authorization or documentation of a waiver or an alteration of Authorization. Limited data sets may be used and disclosed if you have a data use agreement for health care operations (if the consumers whose PHI is affected have executed joint consents) or for research, or public health, public interest, or public benefit as described in Section 3. Network participants may use and disclose a limited data set for research activities conducted by itself, another covered entity, or a researcher who is not a covered entity if the disclosing Network participant and the limited data set recipient enter into a data use agreement. Because limited data sets may contain identifiable information, they are still PHI.

*Limited Data Set* – Refers to PHI that excludes 16 categories of direct identifiers and may be used or disclosed, for purposes of research, public health, or health care operations, without obtaining either an individual's Authorization or a waiver or an alteration of Authorization for its use and disclosure, with a data use agreement.

*Data Use Agreement* – An agreement into which the Network participant enters with the intended recipient of a limited data set that establishes the ways in which the information in the limited data set may be used and how it will be protected.

A limited data set is described as health information that excludes certain, listed direct identifiers (see below) but that may include city; state; ZIP Code; elements of date; and other numbers, characteristics, or codes not listed as direct identifiers. The direct identifiers listed in the HIPAA Privacy Rules' limited data set provisions apply both to information about the individual and to information about the individual's relatives, employers, or household members. The following identifiers must be removed from health information if the data are to qualify as a limited data set:

- |  |  |
|--|--|
| 1. Names.  | 10. Certificate/license numbers.   |
| 2. Postal address information, other than town or city, state, and ZIP Code. | 11. Vehicle identifiers and serial numbers, including license plate numbers. |
| 3. Telephone numbers.  | 12. Device identifiers and serial numbers.                                   |
| 4. Fax numbers.  | 13. Web universal resource locators (URLs).                                  |
| 5. Electronic mail addresses.  | 14. Internet protocol (IP) address numbers.                                  |
| 6. Social security numbers.  | 15. Biometric identifiers, including fingerprints and voiceprints.           |
| 7. Medical record numbers.   | 16. Full-face photographic images and any comparable images.                 |
| 8. Health plan beneficiary numbers.  |  |
| 9. Account numbers.  |  |

JUL 16 2003

A data use agreement is the means by which Network participants obtain satisfactory assurances that the recipient of the limited data set will use or disclose the PHI in the data set only for specified purposes. Even if the person requesting a limited data set from a Network participant is an employee or otherwise a member of the Network participant's workforce, a written data use agreement meeting the HIPAA Privacy Rules' requirements must be in place between the Network participant and the limited data set recipient.

The HIPAA Privacy Rules require that a data use agreement contain the following provisions:

- Specific permitted uses and disclosures of the limited data set by the recipient consistent with the purpose for which it was disclosed (a data use agreement cannot authorize the recipient to use or further disclose the information in a way that would violate the HIPAA Privacy Rules).
- Identify who is permitted to use or receive the limited data set.
- Stipulations that the recipient will:
  - Not use or disclose the information other than permitted by the agreement or otherwise required by law.
  - Use appropriate safeguards to prevent the use or disclosure of the information, except as provided for in the agreement, and require the recipient to report to the Network participant any uses or disclosures in violation of the agreement of which the recipient becomes aware.
  - Hold any agent of the recipient (including subcontractors) to the standards, restrictions, and conditions stated in the data use agreement with respect to the information.
  - Not identify the information or contact the individuals.

If a covered entity is the recipient of a limited data set and violates the data use agreement, it is deemed to have violated the HIPAA Privacy Rules. If the Network participant providing the limited data set knows of a pattern of activity or practice by the recipient that constitutes a material breach or violation of the data use agreement, the Network participant must take reasonable steps to correct the inappropriate activity or practice. If the steps are not successful, the Network participant must discontinue disclosure of PHI to the recipient and notify HHS.

There are specific PHI uses and disclosures that a Network participant is permitted to make for research without an Authorization, a waiver or an alteration of Authorization, or a data use agreement. These limited activities are the use or disclosure of PHI preparatory to research and the use or disclosure of PHI pertaining to decedents for research.

Any questions from DMH staff regarding limited data sets should be directed to the DMH Privacy Officer or designee.

FORM 13-Data Use Agreement contains the mandatory terms that the HIPAA Privacy Rules require to be in a data use agreement.

**Procedure.** Submit the proposed data use agreement to your Privacy Officer or designee for approval. If approved, obtain the signature of the intended recipient

JUL 16 2003

on the data use agreement before disclosing the limited data set. Send the original, signed data use agreement to your Privacy Officer or designee. Retain a copy for your agency's file.

**Minimum Necessary.** A limited data set may contain only the minimum necessary PHI for the purpose for which the limited data set is to be used or disclosed.

**14b) De-Identified Health Information.**

**(1) De-Identified Health Information.**

De-identified information is PHI that has been stripped of all identifiers and cannot be used alone or in combination with any other information to identify the consumer.

De-identified health information may be disclosed without restriction. We will treat as PHI any key or other means to re-identify health information that has been de-identified. Minimum necessary does not apply to de-identified PHI.

We may also disclose PHI to a business associate to create de-identified health information (See Section 13).

The following identifiers must be removed from health information if the data are to qualify as de-identified health information:

1. Names;
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
  - (a) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
  - (b) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;

JUL 16 2003

11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and

18. Any other unique identifying number, characteristic, or code, except that DMH may assign a code or other means of record identification to allow information de-identified to be re-identified by DMH, provided that:

- (a) Derivation. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and
- (b) Security. DMH does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

**Procedure.**

- (1) All identifiers of the consumer and the consumer's relatives, household members, and employers, associated with the health information must be removed. We must have no actual knowledge that the information remaining after stripping these identifiers could be used, alone or in combination with other information to identify the consumer.
- (2) Health information may be de-identified under the supervision and subject to the documented approval of your Privacy Officer or designee.
- (3) Your Privacy Officer or designee must verify that health information is de-identified before you may use or disclose it without restriction.

**(2) Re-Identification Codes.**

Any code or means employed to permit re-identification of de-identified health information will not be derived from or relate to any consumer whose information has been de-identified, be capable of translation to identify a consumer, or be used or disclosed for any purpose other than re-identification of de-identified health information.

**Procedure.** Your Privacy Officer or designee must approve the selection of re-identification codes for de-identified health information. You will consider re-identification codes to be PHI and apply the privacy protections of these Privacy Policies and Procedures to them.

# **RESEARCH – SECTION 15**

**(RESERVED)**

**JUL 16 2003**

## VI. CONSUMER COMPLAINTS

### 16. Complaints and HHS Enforcement.

#### 16a) Complaints.

Your Privacy Officer or designee will investigate and appropriately respond to each written complaint received regarding our compliance with these Privacy Policies and Procedures or the HIPAA Privacy Rules, within ten (10) business days of receipt.

Complaint, for the purposes of this policy, means any concern communicated by a person questioning any act or failure to act relating to a consumer's rights to access to his/her health information, to maintain the privacy of his/her health information, to request restrictions on uses or disclosures of his/her PHI, to request confidential communications regarding his/her PHI, to request amendment of his/her PHI, or to receive an accounting of disclosures of his/her PHI.

#### Procedure.

##### (1) Complaint Receipt.

- Complete, or have the complainant complete, the first and second pages of FORM 14–Complaint.
- Advise the consumer or personal representative of the right to file a grievance.
- If requested, refer the consumer to the group established by your agency to handle grievances.  
(Consumers may also file a grievance with the DMH where appropriate.)
- Promptly transmit the entire FORM 14 to your Privacy Officer or designee.

(2) Complaint Response. Your Privacy Officer or designee will respond to the complaint on your organization's behalf and will process the complaint as follows:

- Forward an information copy of each complaint to the group designated by your agency to handle grievances (and coordinate with them if necessary),
- Investigate the complaint,
- Document the investigation, findings, and conclusions on page 3 of Form 14,
- Notify the complainant of the resolution of the complaint in writing,
- Institute corrective action if warranted, and
- Have the completed FORM 14 and notification letter included in the consumer's clinical record, provide a copy to the consumer, and retain a copy for the Privacy Officer or designee file.

Sample notification letter is attached to Form 14 at the back of this manual.

JUL 16 2003

**16b) Department of Health and Human Services (HHS) Enforcement and Compliance Cooperation.**

Network participants will cooperate with any compliance review or complaint investigation by HHS, while preserving the rights of their organization.

**Procedure.**

**(1) Your Privacy Officer or designee will:**

- Coordinate your response to any HHS compliance review, complaint investigation or other inquiry, to ensure that all applicable obligations of your organization are fulfilled and all applicable rights and privileges of your organization are preserved and protected.
- Arrange for HHS to have access to your facilities, books, records, accounts, and other non-privileged information sources, during normal business hours.

**(2) Agencies.**

- Immediately notify your local Privacy Officer of any inquiry from HHS or any other government official. Your Privacy Officer will inform the DMH Privacy Officer.
- You must await instruction from your local Privacy Officer before responding to these inquiries or providing any documents or other information on behalf of our organization.
- Do not obstruct or interfere with any lawful process, warrant, order or subpoena that may be presented. If the officials insist they have the right of immediate search and seizure of your organization's records, equipment or other matters specified in the process presented, do not obstruct or interfere with them. Instead, use your best efforts to contact your Privacy Officer and to observe and document everything that the officials search, seize, say, and do.

**(3) Verification.** Use Form 4 to verify the identity and authority of a HHS representative prior to disclosure (See Section 5).

**(4) Minimum Necessary.** You are not required to limit PHI to the minimum necessary.

**(5) Disclosure Log.** Use Form 6-Disclosure Log, to document disclosure.

JUL 16 2003

## **VII. SECURITY POLICIES AND PROCEDURES**

These security policies and procedures in some instances speak specifically to DMH responsibilities and to DMH equipment. However, all Network participants shall adopt and follow these security policies to the fullest extent that they are applicable, or they shall adopt and follow comparable security policies and procedures that capture the intent and security measures addressed in these policies.

1. FAX Policy
2. Computer Security
3. Portable Devices Policy
4. Protection and Physical Security of PHI and DMH Sensitive Information
5. Antivirus and Malicious Code Software and Other Requirements
6. DMH Network Security

Security policies on other topics continue to be developed, including specific policies to address security administrative procedures to guard data integrity, confidentiality, and availability of PHI. As these policies are completed they will be disseminated to the Network.

## FAX Policy

### **Purpose.**

To ensure that only authorized persons send and receive DMH sensitive information and protected health information (PHI) by fax, and that appropriate protections are in place to prevent misuse.

### **Policy.**

**Who is Affected:** All DMH (Authority, CSA, Saint Elizabeths Hospital) employees, contractors, and consultants.

**Affected Systems:** All fax systems, including stand-alone fax machines, automatic faxing systems, and computer based faxing systems owned or operated by DMH.

**Location of fax machines:** Fax machines must be located in secured areas where access is available only to authorized or supervised individuals.

**Faxing precautions:** PHI or DMH sensitive information may be faxed only to verified fax numbers. Preprogramming into fax machines is the preferred method. Requests to send faxes to unknown fax numbers should be carefully verified (e.g., contacting the intended recipient in advance or other knowledgeable person) to ensure appropriate authorization. Fax numbers that are entered manually must be double-checked when the fax number is provided and checked again to be certain the correct fax number has been entered before the fax is sent.

**Fax Confidentiality Notice:** All faxes containing PHI must include a confidentiality notice on the cover page advising an inadvertent recipient of the nature of the information and what to do. Sample notice:

The documents accompanying this transmission contain confidential health information that is legally privileged. This information is intended only for the use of the individual or entity named above. The authorized recipient of this information is prohibited from disclosing this information to any other party unless required to do so by law or regulation and is required to destroy the information after its stated need has been fulfilled.

If you are NOT the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this information in error, please notify the sender immediately and arrange for the return or destruction of these documents.

JUL 16 2003

## Computer Security

### Purpose.

Personal computers at the Department of Mental Health are used to acquire, access, process, and manipulate data, including DMH sensitive data and protected health information (PHI). Maintaining appropriate confidentiality of information is a department requirement. Security procedures outlined in this policy must be followed to achieve this goal.

### Policy.

**Who is Affected:** All DMH (Authority, CSA, Saint Elizabeths Hospital) employees, contractors, and consultants.

**Affected Systems:** All personal computers and portable devices owned or operated by DMH. This policy also applies to personal computers and portable devices owned by individuals who maintain confidential information or PHI on them.

**User ID/Passwords:** Access privileges are determined based on the duties and responsibilities of each position. User-specific IDs and passwords for network and application access must be used. Sharing of IDs/passwords is prohibited. Violation of this procedure will result in suspension or termination of network access and privileges. Users are responsible for activity accomplished under their login ID and password.

User ID/passwords are requested by submitting an Information Services Clearance Form to the Information Services Help Desk. Upon approval, user ID/passwords are created or granted. Staff who need additional access or are having problems with their current access should contact their supervisor. The supervisor will complete the necessary Information Services Clearance Form and forward it to the Information Services Help Desk.

**Screensavers:** Use of a screensaver or blank screen which locks the personal computer after a brief period of inactivity is mandatory. Screensavers must be configured to require a password to return to applications or desktop. Recommended interval is fifteen (15) minutes of inactivity before the screen locks.

**Files Downloads:** Only business related files may be saved on computer systems without approval by Information Services. Refer to DMH Policy 686.2, Internet Access and Acceptable Use Policy for details. Care is to be taken when downloading files from email attachments and/or Internet sites. Scanning of downloads for viruses and malicious code may not capture every type of potential problem. Users should be very wary of downloading information from unfamiliar sites.

**Email concerns:** The DMH's electronic-mail system is intended for business purposes. Personal use is permissible only within reasonable limits and in accordance with the guidelines of DMH Policy 686.1, Electronic Mail Acceptable Use Policy. See that policy for details. Any employee who violates this policy will be subject to disciplinary action up to and including termination. DMH policy requires care when dealing with sensitive or PHI to ensure it is properly addressed.

JUL 1 6 2003

Be cautious opening email from unknown parties or with "teaser" lines that are intended to fool users into installing virus or malicious code. Attachments are especially dangerous if they are executable files.

**Social engineering:** A frequently used and very effective method used by those attempting to gain unauthorized access to systems is called social engineering. This technique uses human nature and the willingness of most people to be helpful to gain information and access to systems. Individuals posing as legitimate or temporary users try to get information such as passwords, login names, and access information. It is inappropriate to give out or share information with individuals who have no need for the information or whose identity has not been confirmed. Participation in surveys regarding information security, computer users, network infrastructure, or any Information Services topic should be declined or referred to the DMH Information Security Officer for participation approval.

**File storage on local disks:** DMH confidential and PHI information may NOT be stored on local disk drives. This information must be stored on network drives so that it can be properly secured and backed up.

**File storage on network drives:** Data owners (persons who created or originated the document or file) are responsible for working with Information Services to ensure users rights to network storage locations are set up and maintained properly. Data owners are responsible for permitting access to their files. Files no longer needed should be deleted on a regular basis using DC Government retention schedules.

**File storage on diskettes or other media:** DMH sensitive and PHI may NOT be stored on diskettes or other electronic media without permission of data owner.

**Disposal of storage media:** In order to maintain confidentiality of information, all users are responsible for ensuring storage media are properly destroyed when no longer used. Disposing of intact media in waste containers is NOT adequate. Contact Information Services Help Desk for proper disposal techniques for the following:

- a. Hard Disks
- b. Magnetic tape
- c. Memory modules
- d. Diskettes and CDs.

**PC\Personal computer power on passwords:** It is DMH policy that power-on passwords (*requires a password to continue boot-up of the computer or device*) are not permitted on network PC\personal computers.

**File passwords:** Password protection available in applications such as Microsoft Word, Microsoft Excel, and Microsoft Access provides minimal security, and is not an adequate method of securing PHI or DMH confidential data files. Contact Information Services for security evaluation and/or risk assessment to determine an adequate method for securing PHI or DMH confidential files.

**Modems:** Use of modems on network systems has many security ramifications. Written approval from Information Services is required prior to modem installation.

JUL 16 2003

**Remote control software:** Use of remote control software on personal computers and portable devices is prohibited without the express written approval of Information Services. If approval is given, Information Services procedures for configuring the security aspects of the remote control software must be followed.

## **Portable Devices Policy**

### **Purpose.**

To describe appropriate use of DMH-owned or operated portable devices. This policy outlines physical security requirements, data security requirements, software requirements, and other security needs.

### **Definition.**

Portable devices are electronic devices that may contain user input, transmitted, or copied data and that are small enough to be considered portable in nature. These devices include laptop/notebook computers, personal digital assistants (PDA), portable disk drives such as Iomega Zip drives and CD drives, removable media, voice recording devices of any type, and cell phones or pagers with data storage capabilities.

### **Policy.**

**Who is Affected:** All DMH (Authority, CSA, Saint Elizabeths Hospital) employees, contractors, and consultants. Employees who deliberately violate this policy will be subject to disciplinary action up to and including termination. This policy applies to all portable devices owned or operated by DMH **and** also to all portable devices owned by employees and consultants of DMH which contain PHI or DMH sensitive information.

**Data Security:** In many cases, the data contained in portable devices is more valuable than the devices themselves. Consequently, it is essential that data on these devices be appropriately protected. Following are some general rules regarding data protection:

1. **Computers and devices must use access controls to restrict access to PHI or DMH sensitive data. Access control must be in the form of user ID's and passwords for the device, passwords on data contained in files or applications residing on the device, or encryption technology.**
2. **Only data authorized for use on a portable device may be stored on that device. Written approval by the responsible Privacy Officer, data owner, and Information Services is required before storing PHI or DMH sensitive data on these devices, whether DMH-owned or personally owned. Data must be removed and appropriate security measures taken to clear traces of the data on the storage media.**
3. **Operating systems that support strong security measures are required. MS Windows 95, and MS Windows 98 have inadequate security. MS Windows NT, 2000, and XP or other operating systems approved by the DMH Information Security Officer are required.**

JUL 1 6 2003

**Physical Security:** All users are responsible for protecting the devices from theft and misuse of PHI data. Devices covered by this policy are portable to various degrees. Proper control must be maintained. The following rules must be followed:

1. Never leave devices unattended in non-secure areas.
2. Never leave devices in unlocked vehicles.
3. Never leave devices in plain sight—store in trunk or covered.
4. Never check devices as baggage.
5. Always secure devices with cable locks or store in secure areas.

**PHI and DMH sensitive data on Personally Owned Devices:** Storage or use of PHI or DMH sensitive data on a personally owned device must be approved by the responsible Privacy Officer, data owner, and Information Services. Special care must be taken to remove all data from personally owned devices when access to the data is no longer approved or required.

**Software Applications:** Only software applications that are properly licensed are to be installed on DMH-owned devices.

**Antivirus software:** All anti-virus capable portable devices must be equipped with antivirus software that is updated with new virus patterns at least monthly. For personally owned anti-virus capable portable devices, it is the responsibility of the owner to ensure this rule is followed. All floppies must be scanned for viruses prior to use.

**Remote access:** Portable devices with network connectivity via dial-in or wireless access must follow the policies defined by OCTO for remote access. Contact the Information Services Helpdesk for additional information on this policy.

## Protection and Physical Security of PHI and DMH Sensitive Information

### Purpose.

To ensure that only authorized individuals have access to DMH sensitive and Protected Health Information (PHI) stored or located outside of information systems and computers.

### Policy.

**Who is Affected:** All DMH (Authority, CSA, Saint Elizabeths Hospital) employees, contractors, and consultants.

**Clinical records.** The clinical records of consumers are always defined as PHI. Procedures for use and disclosure are outlined in DMH Privacy Policies and Procedures and in local provider policies. Clinical record storage areas must be tightly controlled locations, provide for signing out of records, and restrict access to the area. Clinical records or portions of those records used in clinical areas must be kept in secure areas when not actually in use. Vigilance in observing that unauthorized individuals do not access clinical records is required on the part of all staff.

**Other Protected Health Information.** Information outside of clinical records that contains individually identifiable data is PHI. This information may be contained in reports, documents, letters, notes, forms, applications, and verbal communication. All PHI, regardless of location, must be treated as confidential and is to be stored, accessed, and transported in a secure manner. Several requirements must be met:

- a. Information is available to authorized individuals.
- b. Locked or secure storage areas must be used.
- c. Documents with PHI must not be posted in public areas.

**Storage and Use of PHI in work areas.** Work areas, including offices, cubicles, shared activity areas, nursing stations, must maintain the confidentiality of PHI. All PHI must be out of view of any casual observer or visitor. PHI must be stored in locked files or desks, or maintained in a tightly controlled access environment.

**Oral Communication.** Communication of PHI via conversation, whether in-person or via electronic communications methods (wired telephone, portable telephone, paging systems, voice mail, telephone answering systems) must use reasonable safeguards to maintain confidentiality. Conversation between clinical staff involving PHI should be discrete and audible only to the involved parties. Paging systems should not communicate PHI under any circumstances. Voice mail messages should minimize disclosure of PHI by requesting a return call to a specific number to a specific person without providing detailed PHI. Messages left on answering systems should provide minimal information, usually requesting a return call.

**Printing.** Reports and documents containing confidential or PHI information must be printed on printers located in secure areas where only authorized individuals can access them. Printouts must be picked up promptly.

JUL 16 2003

**Disposal.** Proper safeguards and procedures must be followed when disposing of PHI and DMH sensitive information after the required record retention time frame has expired. Shredding of PHI and DMH sensitive information must be handled in a secure and appropriate manner.

**Transport of PHI and DMH Sensitive information.** Appropriate procedures and precautions must be used when transferring confidential and PHI information. At a minimum, sealing of envelopes, boxes, or pouches is required, and they should be marked CONFIDENTIAL.

**Identification Badges.** PHI or DMH sensitive information should not be handled or given to any individual without proper identification and authorization. All DMH employees must wear their ID badge at all times when accessing or coming into contact with PHI.

JUL 16 2003

## **Antivirus and Malicious Code Software And Other Requirements**

### **Purpose.**

To prevent occurrences of computer viruses and malicious code incidents. Computer viruses and malicious code incidents pose a serious threat to information security, including availability of network services. Potential effects include: corruption of data; destruction of data; transfer or compromise of confidential or sensitive information; computer operating system problems; increased expenses to repair or correct computer problems; lost productivity; and increased help desk calls. For this reason, efforts to control computer viruses are important at DMH.

### **Definitions.**

1. **Malicious Code**, such as viruses and worms, attack a system in one of two ways, either internally or externally. Traditionally, the virus has been an internal threat, while the worm, to a large extent, has been a threat from an external source.
2. **Computer Viruses** have the following necessary characteristics: replication; requires a host program as a carrier; activated by external action; and replication limited to (virtual) system. In essence, a computer program which has been infected by a virus has been converted into a Trojan horse. The program is expected to perform a useful function, but has the unintended side effect of viral code execution. Upon execution, the virus attempts to replicate and "attach" itself to another program. It is the unexpected and generally uncontrollable replication that makes viruses so dangerous.

### **Policy.**

1. **Computer Hardware:** All personal computers including portable devices are required to have antivirus/malicious code software installed when connected to the DMH network. This includes personally owned equipment. DMH provides the software where deemed appropriate.
2. **Configuration of Antivirus Software:** Procedures for installation and configuration of antivirus software, as determined by Information Services and the DMH Information Security Officer, must be adhered to. Only DMH approved antivirus software may be installed on DMH equipment.
3. **Scanning Features:** All diskettes, CDs, and other media must be scanned by all users prior to use in a personal computer or portable device. All personal computers should be scanned at least weekly for viruses and malicious code. Depending on risk analysis for individual systems, executable files (files that run a program), documents, and other types of files should be considered for scanning before each use.
4. **Reporting Viruses and Malicious Code:** All users should report unusual computer functioning and application problems to the Information Services Help Desk. These may indicate presence of viruses or malicious code.
5. **Virus Alert:** Users who are notified about computer viruses or malicious code via email, various news sources, or via other sources should absolutely NOT forward these messages to

**JUL 1 6 2003**

other users as the email may suggest. Contact the Information Services Help Desk for instructions. In most cases, such emails are actually virus hoaxes relating to non-existent problems. However, virus hoaxes can cause considerable loss in productivity and damage. The Information Services Help Desk will verify and determine the appropriate course of action.

**6. Virus Signature Updates:** Office of the Chief Technology Officer provides DMH automatic updates to virus signatures and patterns. DMH will distribute and update within the network infrastructure as frequently as possible, at a minimum once per week. In the event of the discovery of significant virus or malicious code threats, updates shall be deployed immediately.

**7. Monitoring:** Information Services is responsible for tracking and monitoring occurrences of viruses and malicious code incidents. The Chief Information Officer and Information Security Officer must be informed by designated DMH staff of major incidents, and may be involved in subsequent investigations.

**8. Servers:** Antivirus and malicious code software shall be installed on all servers by Information Services. Configuration, updates, and scanning frequency are determined by Information Services and the Information Security Officer.

**JUL 16 2003**

## DMH Network Security

### **Purpose.**

The security of the DMH network is the foundation for security of electronic information. In order to ensure confidentiality, integrity, and availability of protected health information (PHI) and DMH sensitive information, this policy establishes a set of basic rules for network use that must be followed by all employees, consultants, contractors, and others with access to the DMH network.

### **Policy.**

1. **Connection of Devices:** Information Services must review and approve all requests to connect computers, printers, and portable devices of any type to the DMH network. End-users are not permitted to connect devices to the network without prior written approval from Information Services.
2. **Moving Network Devices:** No devices connected to the DMH network may be relocated and reconnected to the DMH network without approval from Information Services. Contact the Information Services Help Desk at 673-7125 for assistance.
3. **Connection Control:** Information Services is responsible for ensuring that only authorized connections are active.
4. **Modems:** Modem use is not permitted on any device in the DMH network infrastructure without written approval from Information Services.
5. **Monitoring:** Software that monitors any network activity must have written approval from Information Services and the DMH Information Security Officer before installation.
6. **Wireless Connections:** Access points for wireless devices must be approved in writing by Information Services and the Information Security Officer.

JUL 16 2003

## VIII. DEFINITIONS

**Administrative information** means a consumer's name, age, sex, address, identifying number or numbers, dates and character of sessions (individual or group), and fees.

**Agency** for purposes of these policies and procedures, includes the Mental Health Authority, core services agencies, St. Elizabeths Hospital and other organizations in the Network.

**Authorization** means a written form signed by a consumer that authorizes the use or disclosure of the consumer's protected health information (1) by Network providers for purposes other than treatment, payment, or health care operations; or (2) by persons or entities other than Network providers for any purpose.

**Business associate:** A person or entity who, on behalf of a covered entity or of an organized health care arrangement, but other than in the capacity of a member of the workforce of such covered entity or arrangement:

(A) Performs, or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

(B) Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

**Consumer** means the person who is the subject of protected health information.

**Covered entity** means: (1) a health plan; (2) a health care clearinghouse; or (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by these policies and procedures. The Mental Health Authority, Saint Elizabeths Hospital, the DC Community Services Agency, and participating Network providers who transmit health information electronically are covered entities.

**Data collector** means a person, other than the consumer, mental health professional and mental health facility who regularly engages, in whole or in part, in the practice of assembling or evaluating consumer protected health information.

**Data Use Agreement** is an agreement into which the covered entity enters with the intended recipient of a limited data set that establishes the ways in which the information in the limited data set may be used and how it will be protected.

JUL 16 2003

**De-identified Information** is protected health information that has been stripped of all identifiers and cannot be used alone or in combination with any other information to identify the consumer.

**Department of Mental Health (“DMH”)** means the District of Columbia Department of Mental Health, the successor-in-interest to the District of Columbia Commission on Mental Health Services. DMH as used herein encompasses the Mental Health Authority and two provider entities operated directly by DMH (the Public Core Services Agency and Saint Elizabeths Hospital).

**Designated record set** means:

- (1) A group of records maintained by or for a covered entity that is:
  - (i) The clinical records and billing records about consumers maintained by or for a covered health care provider;
  - (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
  - (iii) Used, in whole or in part, by or for the covered entity to make decisions about consumers.
- (2) For purposes of this paragraph, the term *record* means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

**Disclosure** means the release of, transfer of, provision of access to, or divulging in any other manner of information outside the entity holding the information.

**HHS** stands for the United States Department of Health and Human Services.

**Health care** means care, services, or supplies related to the health of a consumer including mental health services and supports. *Health care* includes, but is not limited to, the following:

- (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of a consumer or that affects the structure or function of the body; and
- (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

**Health care clearinghouse** means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and “value-added” networks and switches, that does either of the following functions:

- (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

JUL 16 2003

- (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

**Health care operations** includes functions such as quality assessment and improvement activities, reviewing competence or qualifications of health care professionals, conducting or arranging for medical review, legal services and auditing functions, business planning and development, and general business and administrative activities.

**Health care provider** means a provider of medical or health services and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

**Health oversight agency** means an agency that is authorized by law to oversee the health care system or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

**Health plan** means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg- 91(a)(2)).

**Information Received in Confidence** is information received from other persons on condition that such information not be disclosed to the consumer or other persons.

**Joint consent** means a written form signed by a consumer that grants permission for participating Network providers to use and disclose protected health information in order to carry out treatment, payment, or health care operations including the provision of mental health services or mental health supports.

**Joint consent process** means a process established by the Department of Mental Health to enable all participating Network providers to rely on a single form in which a consumer consents to the use of his or her protected health information by Network providers for the purposes of treatment, payment, and health care operations.

**Law enforcement official** means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

- (1) Investigate or conduct an official inquiry into a potential violation of law; or
- (2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

**Limited Data Set** refers to PHI that excludes 16 categories of direct identifiers and may be used or disclosed, for purposes of research, public health, or health care operations, without obtaining either an individual's Authorization or a waiver or an alteration of Authorization for its use and disclosure, with a data use agreement.

**Mental health facility** means any hospital, clinic, office, nursing home, infirmary, or similar entity where professional services are provided; and any individual or entity that is licensed or

certified by, or has entered into an agreement with DMH to provide mental health services or supports.

***Mental health professional*** means any of the following persons engaged in the provision of professional services: (a) a person licensed to practice medicine; (b) a person licensed to practice psychology; (c) a licensed social worker; (d) a professional marriage, family, or child counselor; (e) a rape crisis or sexual abuse counselor who has undergone at least 40 hours of training and is under the supervision of a licensed social worker, nurse, psychiatrist, psychologist, or psychotherapist; (f) a licensed nurse who is a professional psychiatric nurse; or (g) any person reasonably believed by the consumer to be one of the foregoing persons.

***Mental health provider or "MH provider"*** means (a) any individual or entity, public or private, that is licensed or certified by DMH to provide mental health services or mental health supports; (b) any individual or entity, public or private, that has entered into an agreement with DMH to provide mental health services or mental health supports; and (c) DMH, including Saint Elizabeths Hospital, the DC Community Services Agency and the Mental Health Authority.

***Network*** means the District of Columbia Mental Health Provider Network, an organized health care arrangement consisting of DMH, and every mental health provider that is certified, licensed, or otherwise regulated by DMH, or has entered into a contract or agreement with DMH for the provision of mental health services or mental health supports.

***Network Provider*** means a mental health provider that participates in the Network. Network providers utilize the joint consent process for authorization to use or disclose protected health information in carrying out the provision of mental health services or mental health supports.

***Organized health care arrangement*** means an organized system of health care, such as the Network, in which the participating providers hold themselves out to the public as participating in a joint arrangement, and either (1) participate in joint activities that include utilization review, in which health care decisions by participating providers are reviewed by other participating providers or by a third party on their behalf; or (2) participate in quality assessment and improvement activities, in which mental health services or mental health supports provided by participating providers are assessed by other participating providers or by a third party on their behalf.

***Participating provider*** means Network Provider.

***Payment*** means activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collections activities, medical necessity determinations and utilization review.

***Protected health information (PHI)*** means any written, recorded, or oral information which either (1) identifies, or could be used to identify, a consumer; or (2) relates to the physical or mental health or condition of a consumer, provision of health care to a consumer, or payment for health care provided to a consumer.

***Psychotherapy Process Notes*** are notes made by a mental health professional documenting or analyzing the contents of conversations during an individual, joint, group, or family therapy or counseling session and maintained in a location separate from the consumer's clinical record. They typically contain intimate personal information, details of fantasies or dreams, process interactions, sensitive information about significant persons in the consumer's life, or the therapist's formulations and speculations.

**Quality Improvement Activities** means the systematic, structured processes designed by the DMH/Network to continuously monitor, analyze, and improve its performance to improve the quality of services to its consumers.

**Required by law** means required by DC Code § 21-586 (concerning financial responsibility for the care of hospitalized persons) or by the compulsory reporting provisions of District or federal law which attempt to promote human health and safety.

**Research** means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

**Treatment** means the provision, coordination, or management of health care and related services, consultation between providers relating to a consumer, or referral of a consumer to another provider for health care.

**Use** means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of protected health information within the entity that maintains the protected health information.

**Workforce** as used in these policies and procedures, means every employee in the Network. It includes public and private employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

# **IX. APPENDIX**

**APPENDIX A – Schedule of Fees - RESERVED**

**APPENDIX B – Minimum Necessary Determination Checklist**

**APPENDIX C – Standard Agency Protocols for Routine or Recurring  
Disclosures - RESERVED**

**APPENDIX D – DMH-HIPAA Forms/Letters**

**APPENDIX E – Privacy Compliance Clause**

**APPENDIX F – Department of Mental Health Designated Record Sets Tool**

**JUL 1 6 2003**

**RESERVED**

**SCHEDULE OF FEES**  
**Being developed**

**JUL 16 2003**

**Minimum Necessary Determination Checklist**

**Instructions:** If you cannot check a box in **Section A, B or C** below, you must apply the criteria in **Section D** to determine whether the disclosure or request is for the minimum necessary protected health information (PHI) to accomplish the purpose.

**Section A—Minimum Necessary Not Applicable**

The disclosure or request is not subject to the minimum necessary limitation because:

- ☐ It involves the consumer who is the subject of the information or the consumer's personal representative.
- ☐ It involves an authorization by a consumer who is the subject of the information or the consumer's personal representative.
- ☐ It involves the Department of Health and Human Services (HHS) for complaint investigation or compliance enforcement or review.
- ☐ It is required by law.
- ☐ It is required for compliance with the HIPAA Administrative Simplification Rules.
- ☐ It involves de-identified information.

**Section B—Reliance on Requester**

We can rely on the request to be for the minimum necessary because the request is from one of the following and such reliance is reasonable under the circumstances:

- ☐ A covered entity or a business associate of a covered entity.
- ☐ A professional who is a member of our workforce or is our business associate providing professional services to us, and who represents that the requested information is the minimum necessary.
- ☐ A public official who represents that the requested information is the minimum necessary.
- ☐ A researcher who presents appropriate documentation or representation for the research.

JUL 16 2003

**Section C—Routine or Recurring Disclosure or Request**

- ☐ The disclosure or request is routine or recurring, as listed in our standard protocols (See Appendix C). The disclosure or request must be for no more than the PHI indicated by the appropriate standard protocol.

**Section D—Standard Criteria for Individual Determination**

The disclosure or request must meet our criteria for minimum necessary as determined by following the actions below:

- ☐ Ascertain the purpose of the disclosure or request.
- ☐ Identify the particular PHI to be disclosed or requested.
- ☐ Determine whether the particular PHI is reasonably related to the purpose for the disclosure or request.
- ☐ Review the categories of PHI established in our standard protocols for routine or recurring disclosures and requests, to determine the classifications and groupings of PHI used by our organization for compliance with the minimum necessary limitation.
- ☐ Determine which of our categories of PHI can reasonably be expected to satisfy the purpose of the disclosure or request. Disclose no more than the PHI contained in the least inclusive of those categories.
- ☐ Determine whether the purpose of the disclosure or request can be accomplished with de-identified health information. If it can, then we may disclose or request only de-identified health information.

JUL 16 2003

**STANDARD AGENCY  
PROTOCOLS FOR ROUTINE OR  
RECURRING DISCLOSURES**

**(RESERVED – BEING DEVELOPED)**

**JUL 16 2003**

## DMH-HIPAA FORMS/LETTERS

Form 1 – Joint Notice of Privacy Practices

Form 2 – Consent

Form 3 - Authorization

Form 4 – Identity and Authority Verification

Form 5 – Reserved

Form 6 – Disclosure Log

Form 7 – Access Request Form

*Letters:* Grant of Access to Records

Denial of Access to Records

Direction to Retrieve Records

Form 8 – Designated Personnel and Record Sets

Form 9 – Amendment Request

*Letters:* Grant of Amendment to Records

Denial of Amendment to Records

Notification to Amend Records

Notification of Record Amendment Denial

Form 10 – Request for Accounting

*Letters:* Disclosure Accounting

Direction to Account for Disclosures

Form 11 – Restriction Request/Termination

*Letters:* Denial of Restriction Request

Agreement to Restriction Request

Notification of Restriction on Protected Health Information

Notice of Termination of Restriction Agreement

Notification of Termination of Restriction Agreement

Form 12 – Confidential Communication Request

*Letters:* Accommodation of Confidential Communication Agreement

Denial of Confidential Communication Request

Notification of Confidential Communication Requirement

Form 13 – Data Use Agreement

Form 14 – Complaint Form

*Letters:* Report on Complaint

Form 15 – Assurance of Preservation of the Confidentiality and Security of  
Protected Health Information

JUL 16 2003



*If you require a Spanish translation, call 1-888-793-4357.  
(Statement above appears in Spanish on the privacy brochure)*

## **Joint Notice of Privacy Practices**

**THIS NOTICE IS EFFECTIVE AS OF APRIL 14, 2003**

If you do not speak and/or read English or if you have a hard time understanding this document, please call 1-888-793-4357 or (202) 561-7000 or TDD: (215) 861-4440 or TTY: (886) 788-4989. A representative will assist you 24 hours a day 7 days a week.

---

**THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU  
MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO  
THIS INFORMATION. PLEASE REVIEW THIS NOTICE CAREFULLY.**

---

The District of Columbia Mental Health Provider Network, also known as "The Network", has prepared this Notice. Network members include the District of Columbia Department of Mental Health and all the providers of mental health services or supports that the Department contracts with or regulates. This includes the Mental Health Authority, the Access Help Line, group homes, community residence facilities, Saint Elizabeths Hospital, and agencies that provide the following treatments and services: diagnosis, assessment, medication, counseling, psychotherapy, community support, case management, assertive or intensive case management, crisis/emergency, rehabilitation, intensive day treatment, and other community based interventions.

This notice tells you how your health information will be used, shared, and protected by the participating Network members. The practices described in this notice apply at all the members' sites, including the Authority's office, the Hospital, "CPEP," the emergency psychiatric clinic, other mental health clinics, drop-in centers, group homes, community residence facilities, and other service sites.

### ***What health information is protected?***

- Any information, whether spoken, written, or electronically recorded;
- Created or received by a participating Network member;
- About your past, current, or future mental or physical health; treatment for a mental or physical condition; or payment for treatment provided to you.

---

**CONSENT FOR USES AND DISCLOSURES OF YOUR HEALTH  
INFORMATION AMONG NETWORK MEMBERS:**

---

With your written consent, Network members will share your health information with each other as necessary to carry out treatment, payment, or health care operations.

***What can be done with my information if I consent to disclose it for purposes of treatment, payment, or healthcare operations?***

**For treatment:** Network members can share your health information with other health care specialists so that you can receive the most appropriate treatment. For example, if the agency that is treating you determines that you need a service that it cannot provide, then your agency could send your health information to another Network provider who can provide the service so that you can receive the treatment you need. Network members may also contact you to provide appointment reminders.

**For payment:** Network members can share information about when and why you were seen, so that they can be paid for treating you. For example, we could send information to Medicaid or to your health insurance company stating when and why you were being treated. They can then pay us to help cover our costs of providing you with treatment.

**For health care operations:** Network members may use your health information for health care operations such as evaluating the quality of services provided or investigating unusual incidents. For example, we may review selected charts every month to monitor the quality of the services being provided.

***Can I revoke my consent?***

Yes. You can revoke your consent. But you must do this in writing and bring it to your agency so that the Network can stop using and disclosing your health information. Network members are permitted to use and disclose your health information based on your consent until we receive your revocation in writing.

---

**USES AND DISCLOSURES OF YOUR HEALTH INFORMATION WITHOUT YOUR  
CONSENT OR AUTHORIZATION:**

---

***Under what circumstances can my information be shared without my consent or authorization?***

Your health information can be shared without your prior consent or authorization in the following situations:

- To meet the mandatory reporting requirements of local or federal laws on human health and safety, including laws that require us to report suspected abuse or neglect
- When a mental health professional believes its necessary to ask for emergency psychiatric hospitalization or to protect you or someone else from serious physical harm

- For health oversight activities such as evaluating programs, and doing audits
- For judicial and administrative proceedings such as in response to a court order
- For research purposes, such as research related to the development of better treatments, provided the research study meets certain privacy requirements
- To meet the requirements of any other local or federal laws that apply to privacy of health information
- At the request of a representative who has the legal right to act for you
- At the request of the U.S. Department of Health and Human Services to investigate complaints that we have violated the privacy laws

---

**ANY OTHER USES AND DISCLOSURES OF YOUR HEALTH INFORMATION  
REQUIRE YOUR PERMISSION:**

---

***Can my health information be used or disclosed for other purposes if I give permission?***

Yes. Your health information can be shared for purposes other than those described above, but only if you give specific permission by signing a form called an authorization. For example, you might give us permission to release your health information to a provider outside of the Network to allow that provider to give you a service or treatment that you need. You have the option of saying that the authorization will remain in effect for any period of time up to 60 days, except in cases where you authorized the disclosure in order to get life insurance or health insurance.

***If I authorize disclosure for other purposes, can I revoke my authorization?***

Yes. Except for insurance cases, you can revoke your authorization anytime during the period of time you originally chose for the authorization to remain in effect. You must do this in writing and bring it to us so that we can stop sharing your health information. The Network is permitted to share your health information based on your authorization until the authorization period you chose runs out or we receive your revocation in writing.

---

**OUR DUTY TO PROTECT YOUR HEALTH INFORMATION:**

---

***What are you required to do to protect my health information?***

All Network members are required by law to protect the privacy of your health information. We are also required to provide you with this Notice of our legal duties and our privacy practices. The Network reserves the right to change the terms contained in this Notice. If we do change the terms of this Notice, all Network members will be required to follow the terms of the changed Notice. At all times we are required to follow the terms of the Joint Notice of Privacy Practices currently in effect.

---

## **YOUR RIGHTS REGARDING YOUR HEALTH INFORMATION:**

---

### ***What rights do I have about my health information?***

- You have the right to see and copy your health information with limited exceptions.
- You have the right to request that your record of health information be amended.
- You have the right to be informed about your health information in a confidential manner that you choose. The manner you choose must be reasonable for us to do.
- You have the right to request that we limit certain uses and disclosures of your health information. Network members do not have to agree to your restrictions, but if we do agree, we must follow the restrictions.
- You have the right to obtain information about disclosures we have made of your health information.
- You have the right to have a paper copy of this Privacy Notice.

### ***What can I do if I wish to exercise my rights, have questions, or want to complain about the use and disclosure of my health information?***

If you wish to exercise your rights, or you have a question or complaint about the use and disclosure of your health information, **you should contact the privacy officer at the agency providing you treatment.** You may also contact one or both of the organizations listed below:

Privacy Officer  
D.C. Department of Mental Health  
64 New York Ave, NE, 4<sup>th</sup> Floor  
Washington, D.C. 20002  
Voice: (202) 673-2200  
Fax: (202) 673-3433  
TTD/TTY: (202) 673-7500  
E-mail: [dmh.privacy@dc.gov](mailto:dmh.privacy@dc.gov)

Privacy Official  
D.C. Office of Health Care Privacy and Confidentiality  
In the Office of the Deputy Mayor for Children Youth,  
Families, and Elders  
1350 Pennsylvania Avenue NW, Suite 307  
Washington, D.C. 20004  
Voice: (202) 727-8001  
Fax: (202) 727-0246  
TTD: (202) 442-5999  
TTY: (202) 727-3323  
E-mail: [dcprivacy@dc.gov](mailto:dcprivacy@dc.gov)

You may also complain to the U. S. Department of Health and Human Services, by sending a written complaint to the following address:

Office for Civil Rights – Region III  
U.S. Department of Health and Human Services  
150 S. Independence Mall West, Suite 372  
Public Ledger Building  
Philadelphia, PA 19106-9111  
Main Line (215) 861-4441  
Hotline (800) 368-1019  
FAX (215) 861-4431  
TDD (215) 861-4440  
TTY: (886) 788-4989  
E-mail: [ocrmail@hhs.gov](mailto:ocrmail@hhs.gov)

**No one may take any action against you for complaining about the use and disclosure of your health information.**

---

**CHANGES TO THIS NOTICE:**

---

We reserve the right to change the terms contained in this Joint Notice of Privacy Practices. If we do change the terms of this Notice, the changes will apply to all health information maintained by us, including health information we created or received before the Notice was changed. We will notify people that we have changed the terms of the Notice by posting it at Network offices and by telling people who call the Access Help Line at 1-888-793-4357 or 202-561-7000. We will also post the changed Notice on the Internet at <http://www.dmh.dc.gov>

**Acknowledgement of Receipt**

I confirm that I have been told about the District of Columbia Mental Health Provider Network's Joint Notice of Privacy Practices, and I have been offered a copy of the Notice.

Signature \_\_\_\_\_ Date \_\_\_\_\_

Please Print Name \_\_\_\_\_ Relationship if other than consumer \_\_\_\_\_

\_\_\_\_\_ I refuse to sign this form.

Comments:

---

---

---

---

Note to Network personnel: If consumer/representative refuses Notice or signature, initial here \_\_\_\_\_.

Date \_\_\_\_\_

Comments:

---

---

---

---

**CONSENT**  
**FOR THE USE AND DISCLOSURE OF**  
**PROTECTED HEALTH INFORMATION**  
**AMONG PARTICIPATING NETWORK PROVIDERS**

*The purpose of this form is to get your consent in writing for the use and disclosure of medical information about you so that we may arrange to provide you with treatment, to get paid for that treatment, and to carry out other healthcare activities. Please read this form carefully and ask any questions you wish.*

*I understand that local and federal laws protect the privacy of my health information. My health information includes any information, past, present, or future, about my mental or physical health; about treatment I receive for a mental or physical condition; or about payment for that treatment.*

*I understand that the District of Columbia Mental Health Provider Network -- which includes the Department of Mental Health and all the providers of mental health treatment and services that the Department contracts with or regulates -- has to follow those laws in using, sharing, and protecting my health information.*

*I understand that, under those laws, the Network members need my consent to use and share my protected health information with each other in order to provide me with treatment, to get paid for my treatment, and to carry out other healthcare activities. By signing this consent form I give them permission to share my information for those purposes.*

*I understand that I have the right to see and keep a copy of the Network's Joint Notice of Privacy Practices before I am asked to sign this consent form. The Joint Notice of Privacy Practices provides a more complete description of when and how the Network members can use and disclose my protected health information under the law.*

*I understand that, even though I give my consent, I have the right to ask that the Network members place certain limits on their use and disclosure of my protected health information. They do not have to agree to those limits, but, if they do agree, they must follow those limits.*

*I understand that I have the right to revoke this consent if I change my mind later, but I must do so in writing and give it to the agency that is providing me treatment or to:*

Department of Mental Health Privacy Officer  
64 New York Avenue, N.E., 4<sup>th</sup> Floor, Washington, D.C. 20002  
Phone: (202) 673-2200 TTD/TTY: (202) 673-7500  
fax: (202) 673-3433 e-mail: [dmh.privacy@dc.gov](mailto:dmh.privacy@dc.gov)

Once they receive my written revocation, the Network members must stop sharing my protected health information. In the meantime, the Department of Mental Health and the participating Network providers are free to share my protected health information with each other in order to treat me, to be paid for my treatment, and to carry out other healthcare activities.

\_\_\_\_\_  
Signature of consumer or personal representative

\_\_\_\_\_  
Date

\_\_\_\_\_  
Print name

\_\_\_\_\_  
If personal representative, specify relationship to consumer

**Authorization  
to Use or Disclose Protected Health Information**

\_\_\_\_\_  
Name of Consumer (type or print)

\_\_\_\_\_  
Identification Number

\_\_\_\_\_  
Address

\_\_\_\_\_  
Date of Birth

\_\_\_\_\_  
City/State/Zip Code

\_\_\_\_\_  
Other name(s) used

**GIVE INFORMATION TO:**

\_\_\_\_\_  
Name/Organization

\_\_\_\_\_  
Address

Phone Number: \_\_\_\_\_ Fax Number: \_\_\_\_\_

**INFORMATION TO BE RELEASED BY:**

\_\_\_\_\_  
Name/Organization:

**INFORMATION TO BE DISCLOSED:** Dates of Service: \_\_\_\_\_ to \_\_\_\_\_

<input type="checkbox"/> Discharge Summary	<input type="checkbox"/> Initial Treatment Plan
<input type="checkbox"/> Assessments (specify type)	<input type="checkbox"/> Laboratory Reports
<input type="checkbox"/> Progress Notes	<input type="checkbox"/> History and Physical
<input type="checkbox"/> Individualized Recovery Plan (IRP)/Individualized Plan of Care (IPC)	<input type="checkbox"/> Entire record
<input type="checkbox"/> Doctor's Orders	<input type="checkbox"/> Medications
<input type="checkbox"/> Other (Please Specify): _____ _____	

**INFORMATION TO BE USED FOR THE FOLLOWING PURPOSE(S):**

---

---

**EXPIRATION:** This authorization will expire on the earlier of the following (complete one or both):

- ☐ On \_\_\_\_/\_\_\_\_/\_\_\_\_ (cannot be more than 60 days from the date of this form)
- ☐ When the following happens (which must relate to the consumer or to the purpose of this request):

---

**RIGHT TO REVOKE:** I understand that I may revoke this authorization at any time by giving written notice to the Contact Office listed below. I understand that revocation of this authorization will *not* affect any action you took before you received my written notice of revocation. I understand that my right to revoke this authorization may be limited if the purpose of this authorization involves applying for health or life insurance.

I revoke this authorization effective \_\_\_\_/\_\_\_\_/\_\_\_\_

\_\_\_\_\_  
Signature of consumer or personal representative and relationship to the consumer

**UNAUTHORIZED DISCLOSURE:**

**The unauthorized disclosure of mental health information violates the provisions of the District of Columbia Mental Health Information Act of 1978. Disclosures may only be made pursuant to a valid authorization by the client, or as provided in titles III or IV of that Act. The Act provides for civil damages and criminal penalties for violations.**

I understand that this information cannot legally be disclosed by the person or organization that received it without my authorization.

**OTHER RIGHTS:**

I understand that I have the right to inspect my record of protected health information. I also understand that I cannot be denied enrollment or services if I decide not to sign this form. However, I may not be able to apply for benefits or renewal of benefits that would help pay for these services.

**SIGNATURE OF CONSUMER OR PERSONAL REPRESENTATIVE:**

I, \_\_\_\_\_, understand that, by signing this form, I am authorizing the use and/or disclosure of the protected health information identified above.

\_\_\_\_\_  
Signature Date: \_\_\_\_\_

\_\_\_\_\_  
Print or type full name

**AUTHORITY TO ACT ON BEHALF OF CONSUMER (check one):**

Self \_\_\_\_\_ Parent \_\_\_\_\_ Legal guardian \_\_\_\_\_ Other (specify): \_\_\_\_\_

Address: \_\_\_\_\_

Phone number: \_\_\_\_\_

**SIGNATURE OF MINOR:**

If the consumer is at least 14 years of age, but under 18 years of age, this authorization is not valid unless the consumer signs in addition to the parent/guardian/other personal representative. A minor of any age may authorize disclosure based on his or her signature alone, if (1) he or she is an emancipated minor, or (2) he or she is receiving treatment or services without a parent or legal guardian giving consent.

\_\_\_\_\_  
Signature of Minor Date: \_\_\_\_\_

\_\_\_\_\_  
Print or type full name Date of Birth: \_\_\_\_\_

Address: \_\_\_\_\_

Phone number: \_\_\_\_\_

**YOU ARE ENTITLED TO A COPY OF THIS AUTHORIZATION**

**Put signed original in the consumer's clinical record**

**Send a copy of this form with the information to be disclosed**

## IDENTITY AND AUTHORITY VERIFICATION

**Purpose:** This form is used to document verification of the identity and authority of a person or entity who is requesting or authorizing disclosure of PHI.

### **Section A: Consumer whose information is to be disclosed.**

Name: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone: \_\_\_\_\_

Identification Number: \_\_\_\_\_

### **Section B: Other persons authorizing disclosure or receiving PHI.**

Name: \_\_\_\_\_

Company, Organization or Government Agency with which the person claims affiliation:

Address: \_\_\_\_\_

Telephone: \_\_\_\_\_ E-mail: \_\_\_\_\_

If person is a personal representative, describe relationship to consumer:

### **Section C: Verification of Identity.**

Always try to obtain a copy of what you relied upon to identify the person. Attach it to this form.

How did you verify the person's identity and/or relationship to the consumer or to the company, organization or government agency?

☐ Personal identification (e.g., driver's license, photo ID). Attach a copy, or describe what you saw:

\_\_\_\_\_

☐ Personal representative status (e.g., identification as parent, guardian, executor, administrator, power of attorney). Attach a copy, or describe what you saw:

\_\_\_\_\_

☐ A court order or subpoena bearing a judge's signature authorizing disclosure of PHI:

\_\_\_\_\_

☐ Government credentials (e.g., badge, identification card, appropriate document on government letterhead). Attach a copy, or describe what you saw:

\_\_\_\_\_

- ☐ Government official's oral representation. State what you were told and why your reliance on it was reasonable in the circumstances.

---

- ☐ Proper documentation from an Institutional Review Board, other appropriate privacy board or the researcher relating to research. Attach a copy of the documentation.

I attest that the above information is correct.

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Print name: \_\_\_\_\_

Title: \_\_\_\_\_

## DISCLOSURE LOG

**Purpose:** This form is used to document each disclosure of protected health information that we make for which we are obligated to account on a consumer's request.

### **SECTION A: Consumer whose protected health information was disclosed.**

Name: \_\_\_\_\_ Maiden/Alias: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone: \_\_\_\_\_ Identification Number: \_\_\_\_\_

### **SECTION B: Disclosure made.**

Disclosure Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

**Name and Address (if known) of Person or Entity to whom the Protected Health Information Was Disclosed:**

\_\_\_\_\_  
\_\_\_\_\_

**Protected Health Information Disclosed:** \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

**Purpose of the Disclosure:** Describe the purpose for disclosing the protected health information, or attach a copy of any written request for the information received from a government agency.

\_\_\_\_\_  
\_\_\_\_\_

### **Repetitive Disclosure:**

☐ Check if this disclosure is one of a series of repetitive accountable disclosures for a single purpose to the same person or entity. State, if known, the date of the first disclosure of the series, and the frequency, periodicity or number of these repetitive disclosures made prior to the disclosure being reported on this form.

\_\_\_\_\_  
\_\_\_\_\_

**\*\*\*For disclosure logging related to Research, see Section 15 of this manual.**

I attest that the above information is correct.

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Print name: \_\_\_\_\_

Title: \_\_\_\_\_

# ACCESS REQUEST FORM

**Purpose:** This form is used to document a Consumer's request to inspect and/or obtain a copy of his or her protected health information in a designated record set that we maintain or that our business associates maintain for us.

## **SECTION A: Consumer requesting access.**

Name: \_\_\_\_\_ Maiden/Alias: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone: \_\_\_\_\_ Identification Number: \_\_\_\_\_

## **TO THE CONSUMER: Please read the following and complete the information requested.**

You have the right to inspect and obtain a copy of your protected health information in our designated record sets. To exercise your right of access, please complete Section B.

## **SECTION B: Protected health information access requested.**

Please specify the records you wish to access: \_\_\_\_\_

~~Please do not sign this form before giving it to the consumer.~~

Do you wish to: ☐ Inspect these records? ☐ Obtain a copy of these records?

We will charge you \$.\_\_\_\_\_ per page to copy these records.

Would you like us to make the records available to you: ☐ On paper? ☐ Electronically?

Do you want us to: ☐ Prepare a summary or an explanation of these records?

We will charge you \$\_\_\_\_\_ for the summary or explanation.

Do you want us to: ☐ Mail the copies? We will charge you for the postage.

Please list the name and address of each person, including yourself or your personal representative, for whom you want us to make a copy. If you want us to provide access to or a copy of your records to any person other than you or your personal representative, you must provide us with a signed authorization. We can supply you with an authorization form.

\_\_\_\_\_  
\_\_\_\_\_

### **Consumer:**

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_

If this request is by a personal representative on behalf of the Consumer, complete the following:

### **Personal Representative:**

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Relationship to Consumer: \_\_\_\_\_

Notary Public (Complete only if this request is submitted by mail) \_\_\_\_\_

**YOU ARE ENTITLED TO A COPY OF THIS REQUEST**

## ACCESS REQUEST ACCESS REQUEST PROCESSING

### **SECTION A: Access request processing—to be completed by Privacy Officer or designee.**

We must respond to an access request within 30 days of its receipt.

Date access request received: \_\_\_\_/\_\_\_\_/\_\_\_\_

Date appropriate departments and business associates directed to search for requested records: \_\_\_\_/\_\_\_\_/\_\_\_\_

Departments directed to search designated record sets for the requested records:

\_\_\_\_\_  
\_\_\_\_\_

Business associates directed to search designated record sets for the requested records:

\_\_\_\_\_  
\_\_\_\_\_

### **SECTION B: Response to access request—to be completed by Privacy Officer or designee.**

☐ Access denied on \_\_\_\_/\_\_\_\_/\_\_\_\_ by transmittal of Denial of Access to Records letter to the Consumer.

Reason for denial: \_\_\_\_\_

☐ Consumer requested review on \_\_\_\_/\_\_\_\_/\_\_\_\_ of licensed Mental Health professional's recommendation to withhold records based on endangerment. Attach sheet explaining disposition on review.

☐ Access granted on \_\_\_\_/\_\_\_\_/\_\_\_\_

☐ Records inspected: \_\_\_\_/\_\_\_\_/\_\_\_\_

☐ Copy supplied: \_\_\_\_/\_\_\_\_/\_\_\_\_

Charges: \$ \_\_\_\_\_ Paid: \_\_\_\_/\_\_\_\_/\_\_\_\_

☐ Summary or explanation provided: \_\_\_\_/\_\_\_\_/\_\_\_\_

Charges: \$ \_\_\_\_\_ Paid: \_\_\_\_/\_\_\_\_/\_\_\_\_

### **SIGNATURE.**

I attest that the above information is correct.

### **Privacy Officer or designee:**

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Print name: \_\_\_\_\_

Title: \_\_\_\_\_

## GRANT OF ACCESS TO RECORDS

{DATE}

{CONSUMER'S NAME}

{CONSUMER'S ADDRESS}

Dear {CONSUMER}:

We are granting all or part of the request that we received from you on \_\_\_\_/\_\_\_\_/\_\_\_\_ to inspect and/or obtain a copy of your records. (If we are denying part of your request, you will receive an additional letter from us identifying the records that you requested that we are not providing and the reasons we are not providing them.)

- ☐ The records you requested are ready for inspection. Please contact {CONTACT PERSON OR OFFICE} at {CONTACT INFORMATION} to schedule the inspection.
- ☐ The records you requested are ready for copying to \_\_\_\_ disk or \_\_\_\_ paper as you asked. The copying charge will be \$ \_\_\_\_\_. Upon receipt of payment of this charge, we will promptly copy the records. Please contact {CONTACT PERSON OR OFFICE} at {CONTACT INFORMATION} to arrange to have the copy picked up by or mailed to the persons you designated on your authorization. We will charge you for the postage if you want us to mail the copy.
- ☐ The summary or explanation of the records you requested is ready. Please pay \$ \_\_\_\_\_, the charge to prepare the summary or explanation, and contact {CONTACT PERSON OR OFFICE} at {CONTACT INFORMATION} to arrange to have the summary or explanation picked up by or mailed to the persons you designated on your authorization. We will charge you for the postage if you want us to mail the summary or explanation.

If you have questions or wish to discuss arrangements, please contact {CONTACT PERSON OR OFFICE} at {CONTACT INFORMATION}

Sincerely,

{ORGANIZATION NAME}

By: \_\_\_\_\_  
Privacy Officer or designee

JUL 16 2003

## DENIAL OF ACCESS TO RECORDS

{DATE}

{CONSUMER'S NAME}

{CONSUMER'S ADDRESS}

Dear {CONSUMER}:

We are denying all or part of the request that we received from you on \_\_\_\_/\_\_\_\_/\_\_\_\_ to inspect and/or obtain a copy of your records. (If we are granting part of your request, you will receive an additional letter from us with instructions for inspecting and/or obtaining a copy of the records we are providing.) The reasons we cannot accommodate your request are:

- ☐ We do not have the requested records.
- ☐ We do not know who may have the requested records.
- ☐ You may be able to obtain the requested records by contacting: \_\_\_\_\_
- ☐ The records you requested were obtained in confidence from a source other than a health care provider, and providing you access to these records is likely to reveal the confidential source.
- ☐ The records were created or obtained in the course of research, and you agreed not to have access to them while the research remains in progress when you gave your authorization to participate in the research.
- ☐ A licensed mental health professional has determined that providing you or your personal representative access to these records is likely to endanger the safety or life of you or another, or that the records contain references to persons not health care providers whose safety or life may be endangered if the access you request were granted.
- ☐ Other: \_\_\_\_\_

If you disagree with the recommendation of the licensed mental health professional, you may designate a different licensed mental health professional who did not participate in the recommendation to deny you access to review that recommendation. Please contact {CONTACT PERSON OR OFFICE} at {CONTACT INFORMATION} to request such a review.

You may file a complaint about our denial of your access request with us or with the United States Department of Health and Human Services. Please contact {CONTACT PERSON OR OFFICE} at {CONTACT INFORMATION} to learn about the procedure for complaining to us or to the Department of Health and Human Services.

If you have questions, wish to discuss the denial or file a complaint, please contact {CONTACT PERSON OR OFFICE} at {CONTACT INFORMATION}.

Sincerely,  
{ORGANIZATION NAME}

By: \_\_\_\_\_  
Privacy Officer or designee

JUL 16 2003

## DIRECTION TO RETRIEVE RECORDS

To: {Business Associate}  
\_\_\_\_\_  
\_\_\_\_\_

From: **{ORGANIZATION NAME}**  
**{PRIVACY OFFICER NAME AND CONTACT INFORMATION}**

On \_\_\_\_/\_\_\_\_/\_\_\_\_, we received a request from the consumer below to inspect and copy the following records:

\_\_\_\_\_  
\_\_\_\_\_

We believe you may have some or all of the requested records in a designated record set. Please promptly search your designated record sets, retrieve each of the requested records you find, and transmit those records to me. If you find none, please check the box below. Please sign and return this form to me.

As we must respond to this request by \_\_\_\_/\_\_\_\_/\_\_\_\_, please give this your immediate attention.

**Privacy Officer or designee:**

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Title: \_\_\_\_\_

**Consumer requesting access:**

Name: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone: \_\_\_\_\_ Identification Number: \_\_\_\_\_

**Response to direction to retrieve records:**

After due search of designated record sets we maintain for you, we:

- ☐ Found no records responsive to the consumer's request.
- ☐ Found the following responsive records and are transmitting these to you:

\_\_\_\_\_  
\_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

(Business Associate Representative)

Title: \_\_\_\_\_

(Business Associate Representative)

**JUL 16 2003**

## DESIGNATED PERSONNEL AND RECORD SETS

**Purpose:** This form is used to document the designation of personnel in your department responsible for compliance with requests for access to, amendment of, and disclosure accounting for a consumer's protected health information. It is also used to document the locations and the paths where your department maintains paper or electronic documentation that makes up your department's designated record sets. Designated record sets include those medical and billing records maintained by your department, or those records that your department uses to make decisions about our consumers.

### **SECTION A: Department.**

Department Name: \_\_\_\_\_

Director: \_\_\_\_\_

Telephone: \_\_\_\_\_ E-mail: \_\_\_\_\_

Location: \_\_\_\_\_

### **SECTION B: Designated personnel.**

The following department personnel or positions are responsible for the department's compliance with requests for access to, amendment of, and disclosure accounting for protected health information in our department's designated record sets:

\_\_\_\_\_  
\_\_\_\_\_

### **SECTION C: Designated record sets.**

The file drawers and room locations of paper documentation that is part of the department's designated record sets:

\_\_\_\_\_  
\_\_\_\_\_

The paths to electronic documentation that is part of the department's designated record sets:

\_\_\_\_\_  
\_\_\_\_\_

An individual's protected health information may best be retrieved from the department's designated record sets by:

- ☐ Individual name  
☐ Identification number  
☐ Other identifiers: \_\_\_\_\_

### **SIGNATURE.**

I attest that the above information is correct.

### **Privacy Officer or designee:**

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Print name: \_\_\_\_\_ Title: \_\_\_\_\_

Original – Local Privacy Officer/Copy – DMH Privacy Officer

# AMENDMENT REQUEST

**Purpose:** This form is used for a Consumer's request to amend protected health information in designated record sets that we maintain or that our business associates maintain for us.

## **SECTION A: Consumer requesting records amendment.**

Name: \_\_\_\_\_ Maiden/Alias: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone: \_\_\_\_\_ Identification Number: \_\_\_\_\_

### **TO THE CONSUMER: Please read the following and complete the information requested.**

You have the right to request us to amend your protected health information in our designated record sets. We may decline your request if the information is not part of our designated record sets, we did not create the information, we believe the information is complete and accurate, and for certain other reasons. To exercise your right to request amendment, please complete Section B.

## **SECTION B: Protected health information to be amended.**

Please specify the records you wish to amend and the amendment you wish to make: \_\_\_\_\_

\_\_\_\_\_

Please state the reason for the amendment: \_\_\_\_\_

\_\_\_\_\_

Please list the name and address of each person who you want us to notify of the amendment, should we agree to make the amendment you request. You must provide us with a signed authorization for us to notify these persons. We can supply you with the appropriate authorization form.

\_\_\_\_\_  
\_\_\_\_\_

### **Consumer:**

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_

If this request is by a personal representative on behalf of the Consumer, complete the following:

### **Personal Representative:**

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Relationship to Consumer: \_\_\_\_\_

Notary Public (Complete only if this request is submitted by mail) \_\_\_\_\_

**YOU ARE ENTITLED TO A COPY OF THIS REQUEST.**

# AMENDMENT REQUEST

## AMENDMENT REQUEST PROCESSING

### **SECTION A: Consumer's amendment request to be completed by Privacy Officer or designee.**

We must respond to a Consumer's amendment request within 60 days.

Date amendment request received: \_\_\_\_/\_\_\_\_/\_\_\_\_ Date transmitted to Privacy Officer: \_\_\_\_/\_\_\_\_/\_\_\_\_

#### **Extension of response date:**

We may take one 30 day extension of our response date by notifying the requester within the original 60 day response period of the reason for the extension and the date on which we will provide our response.

Extension notice sent on: \_\_\_\_/\_\_\_\_/\_\_\_\_ Response date promised in extension notice: \_\_\_\_/\_\_\_\_/\_\_\_\_

Reason given for extension: \_\_\_\_\_

### **SECTION B: Response to Consumer's amendment request.**

☐ Amendment denied on \_\_\_\_/\_\_\_\_/\_\_\_\_ by transmittal of Denial of Amendment to Records letter to the Consumer.

☐ Consumer requested on \_\_\_\_/\_\_\_\_/\_\_\_\_ that the amendment request and our denial be included in future disclosures of the record. Notify departments and business associates listed below to append or link the amendment request and our denial, and any accurate summary of them that the Privacy Officer prepared, to the record for inclusion with future disclosures.

☐ Consumer submitted written disagreement on \_\_\_\_/\_\_\_\_/\_\_\_\_. Attach written disagreement and notify departments and business associates listed below to append or link the written disagreement, and any accurate summary of it that the Privacy Officer prepared, to the record for inclusion with future disclosures.

☐ We prepared rebuttal to Consumer's written disagreement and sent it to the Consumer on \_\_\_\_/\_\_\_\_/\_\_\_\_. Attach rebuttal and notify departments and business associates listed below to append or link the rebuttal, and any accurate summary that the Privacy Officer prepared of the Consumer's written disagreement and the rebuttal, to the record for inclusion with future disclosures.

☐ Consumer lodged a complaint on \_\_\_\_/\_\_\_\_/\_\_\_\_.

☐ Amendment granted on \_\_\_\_/\_\_\_\_/\_\_\_\_ by transmittal to the Consumer. Notify departments, business associates, persons that the Consumer has authorized to receive notice, and others who we know have and may rely on the unamended records to the Consumer's detriment, as listed below, to amend the records.

Departments, business associates and others to be notified of the grant or denial of the request to amend:

\_\_\_\_\_

I attest that the above information is correct.

#### **Privacy Officer or designee:**

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Print name: \_\_\_\_\_

Title: \_\_\_\_\_

## GRANT OF AMENDMENT TO RECORDS

{DATE}

{CONSUMER'S NAME}

{CONSUMER'S ADDRESS}

Dear {CONSUMER}:

We are granting the request that we received from you on \_\_\_\_/\_\_\_\_/\_\_\_\_ to amend your records. We have amended our designated record sets to reflect the amendment, and have notified our business associates and others as appropriate of the amendment. We have also notified the persons for whom you provided a signed authorization allowing us to give notice that your records have been amended.

If you have questions please contact {CONTACT PERSON OR OFFICE} at {CONTACT INFORMATION}.

Sincerely,

{ORGANIZATION NAME}

By: \_\_\_\_\_  
Privacy Officer or designee

JUL 16 2003

## DENIAL OF AMENDMENT TO RECORDS

{DATE}

{CONSUMER'S NAME}

{CONSUMER'S ADDRESS}

Dear {INDIVIDUAL}:

We are denying the request that we received from you on \_\_\_\_/\_\_\_\_/\_\_\_\_ to amend your records. The reasons we have determined that your request should be denied are:

- ☐ We do not have the records you wish to amend in our designated record sets.
- ☐ We did not create the records you wish to amend, and we have no basis to believe that the person or entity that did create the records is available to amend them.
- ☐ We believe the records you wish to amend are complete and accurate.
- ☐ Other: \_\_\_\_\_

Your options:

1. You may submit a written statement disagreeing with our decision. If you do, we will append or link your statement to the records you wanted to amend (if we have those records in our designated record sets) for inclusion in future disclosures of those records. We may prepare and send you a rebuttal to your statement. If we do, we will append or link our rebuttal to those same records for inclusion in future disclosures of those records. In the alternative, we may substitute an accurate summary of your written statement and our rebuttal with future disclosures of those records.
2. Instead of submitting a written statement of disagreement, you may ask that your request to amend the records and this denial be appended or linked to those records to be included with future disclosures. We may substitute an accurate summary of your request and this denial with future disclosures.
3. You may file a complaint about our denial of your amendment request with us or with the United States Department of Health and Human Services. Please contact {CONTACT PERSON OR OFFICE} at {CONTACT INFORMATION} to learn about the procedure for complaining to us or to the Department of Health and Human Services.

If you have questions, wish to discuss the denial, file a complaint or review your options, please contact {CONTACT PERSON OR OFFICE} at {CONTACT INFORMATION}.

Sincerely,

{ORGANIZATION NAME}

By: \_\_\_\_\_  
Privacy Officer or designee

JUL 16 2003

## NOTIFICATION TO AMEND RECORDS

To: {Business Associate}

From: {ORGANIZATION NAME}  
{PRIVACY OFFICER NAME AND CONTACT INFORMATION}

On \_\_\_\_/\_\_\_\_/\_\_\_\_, we granted a request from the consumer below or received notice from the covered entity below to amend the following records with the information attached to this letter:

\_\_\_\_\_  
\_\_\_\_\_  
We believe you may have these records in a designated record set you maintain for us. If so, please promptly amend the records by appending the attached amendment to them. Please contact me should you have questions about the amendment.

Sincerely,  
{ORGANIZATION NAME}

\_\_\_\_\_  
Privacy Officer or designee

Date: \_\_\_\_\_

**Consumer requesting or covered entity issuing notice to amend record:**

Name: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone: \_\_\_\_\_ Identification Number: \_\_\_\_\_

JUL 16 2003

## NOTIFICATION OF RECORD AMENDMENT DENIAL

To: {Business Associate}

From: { ORGANIZATION NAME}  
{PRIVACY OFFICER NAME AND CONTACT INFORMATION}

On \_\_\_\_/\_\_\_\_/\_\_\_\_, we denied a request from the consumer below to amend the following records:

- \_\_\_\_\_
- \_\_\_\_\_
- ☐ The consumer's request to amend these records and our denial are attached.
  - ☐ The consumer submitted a written statement disagreeing with our denial. It is attached along with any rebuttal we prepared.
  - ☐ Attached is an accurate summary of the consumer's request, our denial, any written statement of disagreement from the consumer, and any rebuttal we prepared.

Please append or link these materials to these records in the designated record sets you maintain for us so they may be included as appropriate in future disclosures of these records.

Please contact me should you have questions.

\_\_\_\_\_  
Privacy Officer or designee

Date: \_\_\_\_\_

**Consumer Requesting Record Amendment:**

Name: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone: \_\_\_\_\_ Identification Number: \_\_\_\_\_

JUL 16 2003

# REQUEST FOR ACCOUNTING

Purpose: This form is used to document a consumer's request for an accounting of disclosures of protected health information that we maintain or that our business associates maintain for us.

## **SECTION A: Consumer requesting disclosure accounting.**

Name: \_\_\_\_\_ Maiden/Alias: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone: \_\_\_\_\_ Identification Number: \_\_\_\_\_

## **SECTION B: To the consumer—Please read the following.**

You have the right to an accounting of the disclosures we or our business associates have made of your protected health information (a) without your permission as allowed by law and (b) to the Department of Health and Human Services for privacy compliance purposes. The accounting period is the 6 years prior to your request, except you are not entitled to an accounting of any disclosures made before April 14, 2003, which is our compliance date under the federal privacy rules.

~~(Privacy Officer or designee of the entity, before giving to consumer)~~

You are entitled to one free disclosure accounting each 12 months. We will charge you \$ \_\_\_\_\_ for each additional disclosure accounting you request during the same 12 month period.

To request a disclosure accounting, please complete the signature block below.

### **Consumer:**

I request an accounting of the accountable disclosures of my protected health information between \_\_\_\_/\_\_\_\_/\_\_\_\_ and \_\_\_\_/\_\_\_\_/\_\_\_\_. I understand that I am entitled to one free disclosure accounting each 12 months. I agree to pay \$ \_\_\_\_\_ for this disclosure accounting if I have already received a disclosure accounting from you within the previous 12 months.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_

If this request is by a personal representative on behalf of the consumer, complete the following:

### **Personal Representative:**

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Relationship to Consumer: \_\_\_\_\_

**YOU ARE ENTITLED TO A COPY OF THIS REQUEST**

# REQUEST FOR ACCOUNTING

## DISCLOSURE ACCOUNTING PROCESSING

### **SECTION A: Disclosure accounting request processing—to be completed by Privacy Officer or Designee.**

We must respond to a disclosure accounting request within 60 days of its receipt.

Date accounting request received: \_\_\_\_/\_\_\_\_/\_\_\_\_ Date transmitted to Privacy Officer or Designee: \_\_\_\_/\_\_\_\_/\_\_\_\_

Accounting period: From: \_\_\_\_/\_\_\_\_/\_\_\_\_ To: \_\_\_\_/\_\_\_\_/\_\_\_\_

Date of last accounting: \_\_\_\_/\_\_\_\_/\_\_\_\_

If last accounting was within 12 months of this request, charge consumer \$\_\_\_\_\_.

Date appropriate departments and business associates directed to account for disclosures: \_\_\_\_/\_\_\_\_/\_\_\_\_

Departments directed to account for disclosures:

\_\_\_\_\_  
\_\_\_\_\_

Business associates directed to account for disclosures:

\_\_\_\_\_  
\_\_\_\_\_

**Extension of response date:**

We may take one 30 day extension of our response date by notifying the requester within the original 60 day response period of the reason for the extension and the date on which we will provide our response.

Extension notice sent on: \_\_\_\_/\_\_\_\_/\_\_\_\_ Response date promised in extension notice: \_\_\_\_/\_\_\_\_/\_\_\_\_

Reason given for extension: \_\_\_\_\_

### **SECTION B: Response to accounting request—to be completed by Privacy Officer or Designee.**

Disclosure accounting delivered on \_\_\_\_/\_\_\_\_/\_\_\_\_ by transmittal of Disclosure Accounting to the consumer.

Charges assessed were \$\_\_\_\_\_.

**Privacy Officer or designee:**

I attest that the above information is correct.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Print name: \_\_\_\_\_ Title: \_\_\_\_\_

## DISCLOSURE ACCOUNTING

{DATE}

{CONSUMER'S NAME}

{CONSUMER'S ADDRESS}

Dear {CONSUMER}:

The accounting you requested on \_\_\_\_/\_\_\_\_/\_\_\_\_ of the disclosures of your protected health information that we or our business associates made between \_\_\_\_/\_\_\_\_/\_\_\_\_ and \_\_\_\_/\_\_\_\_/\_\_\_\_ is {ready/enclosed}. {Because you have already received a disclosure accounting from us within the last 12 months, we are entitled to charge you for this disclosure accounting. The charge is \$ \_\_\_\_\_. Upon receipt of payment, we will send the disclosure accounting to you.}

The disclosure accounting does not include disclosures we or our business associates made before April 14, 2003, which is our compliance date under federal privacy rules.

We have provided for each accountable disclosure (a) the disclosure date, (b) the name and (if known) address of the person or entity to which the disclosure was made, (c) a description of the protected health information disclosed, and (d) the purpose for which the protected health information was disclosed. For repetitive disclosures during the accounting period to the same person or entity for a single purpose, we have provided (a) the frequency, periodicity or number of these repetitive disclosures during the accounting period, and (b) the date of the last of these repetitive disclosures during the accounting period.

If you have questions regarding the disclosure accounting, please contact {CONTACT PERSON OR OFFICE} at {CONTACT INFORMATION}

Sincerely,

{ORGANIZATION NAME}

By: \_\_\_\_\_  
Privacy Officer or designee

JUL 16 2003

## DIRECTION TO ACCOUNT FOR DISCLOSURES

To: {Business Associate} \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

From: {ORGANIZATION NAME}  
{PRIVACY OFFICER NAME AND CONTACT INFORMATION}

On \_\_\_\_/\_\_\_\_/\_\_\_\_, we received a request from the consumer below for an accounting of the disclosures of the consumer's protected health information made between \_\_\_\_/\_\_\_\_/\_\_\_\_ and \_\_\_\_/\_\_\_\_/\_\_\_\_ (the "accounting period"). Please promptly provide us with an accounting of each disclosure of this consumer's protected health information you have made within the accounting period.

We do not have to account for disclosures that are exempt from accounting as follows: (a) disclosures made before April 14, 2003, (b) disclosures made within the Network for treatment, payment, or health care operations, (c) disclosures made to the consumer or the consumer's personal representative, (d) disclosures made pursuant to authorization, (e) disclosures made as part of a limited data set, (f) disclosures of de-identified PHI, (g) disclosures to business associates, (h) disclosures that are for national security or intelligence purposes, and (i) disclosures made to correctional institutions or other law enforcement officials having lawful custody over an individual.

For each accountable disclosure, please provide (a) the disclosure date, (b) the name and (if known) address of the person or entity to which the disclosure was made, (c) a description of the protected health information disclosed, and (d) the purpose for which the protected health information was disclosed.

For repetitive disclosures during the accounting period to the same person or entity for a single purpose, you may provide (a) the frequency, periodicity or number of these repetitive disclosures during the accounting period, and (b) the date of the last of these repetitive disclosures during the accounting period.

As we must provide the disclosure accounting by \_\_\_\_/\_\_\_\_/\_\_\_\_, please give this your immediate attention. Please contact me should you have questions or wish to discuss this request for disclosure information.

**Privacy Officer or designee:**

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Title: \_\_\_\_\_

**Consumer requesting disclosure accounting:**

Name: \_\_\_\_\_ Maiden/Alias: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone: \_\_\_\_\_ Identification Number: \_\_\_\_\_

**JUL 1 6 2003**

## RESTRICTION REQUEST/TERMINATION

**Purpose:** This form is used for a consumer's request to restrict our use or disclosure of protected health information for treatment, payment or health care operations, or with specified persons involved with the consumer's care or payment for care.

### **SECTION A: Consumer requesting restriction.**

Name: \_\_\_\_\_ Maiden/Alias: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone: \_\_\_\_\_ Identification Number: \_\_\_\_\_

### **TO THE CONSUMER: Please read the following and complete the information requested.**

You have the right to request that we restrict our use or disclosure of your protected health information for treatment, payment or health care operations or with persons involved in your care or payment for your care. We will do our best to honor your request. If we do, our agreement must be in writing. We will then restrict our use or disclosure of your protected health information as you request. We may, notwithstanding our agreement, use or disclose the restricted information when needed to treat you in a medical/psychiatric emergency, or when required or authorized by law.

You may end a restriction agreement at any time by notifying us in writing. Your protected health information will then no longer be subject to the restriction. To exercise your right to request restriction on our use or disclosure of your protected health information, please complete Section B.

### **SECTION B: Restriction requested.**

Please specify the protected health information, the use or disclosure of which you want to restrict:

\_\_\_\_\_  
\_\_\_\_\_

Please state the restriction you want to apply to that protected health information:

\_\_\_\_\_  
\_\_\_\_\_

### **Consumer:**

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_

If this request is by a personal representative on behalf of the consumer, complete the following:

### **Personal Representative:**

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Relationship to Consumer: \_\_\_\_\_

YOU ARE ENTITLED TO A COPY OF THIS REQUEST

## RESTRICTION REQUEST/TERMINATION

### SECTION C: Termination of Restriction Agreement.

Reason restriction agreement is being terminated:

---

---

---

**Consumer:**

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Print name: \_\_\_\_\_

If this request is by a personal representative on behalf of the consumer, complete the following:

**Personal Representative:**

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Relationship to Consumer: \_\_\_\_\_

# RESTRICTION REQUEST/TERMINATION

## RESTRICTION REQUEST PROCESSING

### **SECTION A: Response to restriction request—to be completed by Privacy Officer or Designee.**

☐ Request denied on \_\_\_\_/\_\_\_\_/\_\_\_\_ by transmittal of Denial of Restriction Request letter to the consumer.

☐ Request granted on \_\_\_\_/\_\_\_\_/\_\_\_\_ by transmittal of Agreement to Restriction Request letter to the consumer.

Departments and business associates notified of the accepted restriction:

\_\_\_\_\_  
\_\_\_\_\_

I attest that the above information is correct.

#### **Privacy Officer or designee:**

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Print name: \_\_\_\_\_

Title: \_\_\_\_\_

### **SECTION B: Termination of Request Processing.**

Notice of Termination of Restriction Agreement sent to the consumer on \_\_\_\_/\_\_\_\_/\_\_\_\_.

Departments and business associates notified of the termination of restriction agreement: (should conform to the list of departments and business associates above.)

\_\_\_\_\_  
\_\_\_\_\_

I attest that the above information is correct.

#### **Privacy Officer or designee:**

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Print name: \_\_\_\_\_

Title: \_\_\_\_\_

## DENIAL OF RESTRICTION REQUEST

{DATE}

{CONSUMER'S NAME}

{CONSUMER'S ADDRESS}

Dear {CONSUMER}:

We decline your \_\_\_\_/\_\_\_\_/\_\_\_\_ request that we restrict our use or disclosure of your protected health information. That means we will be permitted to use or disclose the protected health information that we create, receive or maintain about you in accordance with our Privacy Practices Notice that we have given to you.

If you have questions or want to discuss the denial of your restriction request, please contact {CONTACT PERSON OR OFFICE} at {CONTACT INFORMATION}.

Sincerely,

{ORGANIZATION NAME}

By: \_\_\_\_\_  
Privacy Officer or designee

JUL 16 2003

## AGREEMENT TO RESTRICTION REQUEST

{DATE}

{CONSUMER'S NAME}

{CONSUMER'S ADDRESS}

Dear {CONSUMER}:

Effective as of \_\_\_\_/\_\_\_\_/\_\_\_\_, we agree to restrict our use or disclosure of your protected health information in accordance with your request received on \_\_\_\_/\_\_\_\_/\_\_\_\_. We will not use or disclose the protected health information you identified in your request contrary to the restriction you requested as long as this agreement remains in effect, *except* we may use or disclose the restricted information in a medical/psychiatric emergency for your treatment, when you authorize us in writing to use or disclose the information, or when the use or disclosure is required or authorized by law.

You may end this restriction agreement at any time by notifying us in writing. Your protected health information will then no longer be subject to the restriction.

If you have questions or wish further information, please contact {CONTACT PERSON OR OFFICE} at {CONTACT INFORMATION}.

Sincerely,

{ORGANIZATION NAME}

By: \_\_\_\_\_  
Privacy Officer or designee

JUL 16 2003

## NOTIFICATION OF RESTRICTION ON PROTECTED HEALTH INFORMATION

To: {Business Associate}

From: {ORGANIZATION NAME}  
{PRIVACY OFFICER NAME AND CONTACT INFORMATION}

On \_\_\_\_/\_\_\_\_/\_\_\_\_, we agreed to a request from the consumer below to restrict our use or disclosure of the following protected health information:

\_\_\_\_\_  
\_\_\_\_\_

The restriction that applies to the above protected health information is:

\_\_\_\_\_  
\_\_\_\_\_

You must ensure that the above protected health information is neither used nor disclosed in violation of the above restriction. Should the restriction be modified or removed, we will notify you in writing. If you have questions, please contact me.

Sincerely,  
{ORGANIZATION NAME}

\_\_\_\_\_  
Privacy Officer or designee

Date: \_\_\_\_\_

### Consumer Requesting Restriction:

Name: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone: \_\_\_\_\_ Identification Number: \_\_\_\_\_

JUL 1 6 2003

## NOTICE OF TERMINATION OF RESTRICTION AGREEMENT

{DATE}

{CONSUMER'S NAME}

{CONSUMER'S ADDRESS}

Dear {CONSUMER}:

Based on your request, we are hereby terminating the agreement we made with you on \_\_\_\_/\_\_\_\_/\_\_\_\_ to restrict our use or disclosure of your protected health information. This termination is effective \_\_\_\_/\_\_\_\_/\_\_\_\_. After this termination effective date, we will no longer subject any protected health information we may create or receive about you to the restriction agreement. Rather, we will be permitted to use or disclose this protected health information in accordance with our Privacy Practices Notice that we have given to you.

Please sign this letter where indicated below and return it to us. Then the restriction you had requested and to which we had agreed will no longer apply to your protected health information created or received previously subject to the restriction. That information will then be treated as any other protected health information we may have about you. Our treatment of your protected health information is explained in our Privacy Practices Notice that we have given to you.

If you have questions or wish further information, please contact {CONTACT PERSON OR OFFICE} at {CONTACT INFORMATION}.

Sincerely,

{ORGANIZATION NAME}

By: \_\_\_\_\_  
Privacy Officer or designee

---

### CONCURRENCE IN TERMINATION OF RESTRICTION AGREEMENT

By signing the termination of our restriction agreement, my protected health information created or received subject to our restriction agreement will no longer be subject to the restriction. I also understand that any protected health information you create or receive about me after the effective date of the termination of our restriction agreement will not be subject to the restriction. Rather, all of my protected health information that you create, receive or maintain will be used or disclosed as explained in your Privacy Practices Notice.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

After you sign and date this concurrence, please return it to {INSERT PRIVACY OFFICER NAME AND ADDRESS}.

JUL 16 2003

## NOTIFICATION OF TERMINATION OF RESTRICTION AGREEMENT

To: {Business Associate}

From: {ORGANIZATION NAME}  
{PRIVACY OFFICER NAME AND CONTACT INFORMATION}

Based on the consumer's request, effective \_\_\_\_/\_\_\_\_/\_\_\_\_ we terminated our agreement with the consumer below to restrict our use or disclosure of the following protected health information:

\_\_\_\_\_  
\_\_\_\_\_

The restriction to which we had agreed with respect to the above protected health information is:

\_\_\_\_\_  
\_\_\_\_\_

If you have questions or wish to discuss the matter, please contact me.

Sincerely,  
{ORGANIZATION NAME}

\_\_\_\_\_  
Privacy Officer or designee

Date: \_\_\_\_\_

**Consumer requesting restriction:**

Name: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone: \_\_\_\_\_ Identification Number: \_\_\_\_\_

**JUL 16 2003**

## Confidential Communication Request

**Purpose:** This form is used for a consumer's request that we use alternative means or an alternative location when communicating about protected health information.

### **SECTION A: Consumer requesting confidential communication.**

Name: \_\_\_\_\_ Maiden/Alias: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone: \_\_\_\_\_ Identification Number: \_\_\_\_\_

### **SECTION B: To the consumer—please read the following and complete the information requested.**

You have the right to request that we communicate about all or part of your protected health information by alternative means or to an alternative location. We will accommodate your request (a) if it is reasonable, and (b) you provide reasonable alternative means or location for communicating with you. To exercise this right, please complete this Section B.

Please describe the protected health information you want to make subject to confidential communication, and also include the reason why if you wish to do so.

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

☐ I request that you communicate with me about my protected health information by the following alternative means. Please provide full information on the alternative means you want us to use:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

☐ I request that you communicate with me about my protected health information at the following alternative location. Please provide full information on the alternative location:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

### **Consumer:**

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_

If this request is by a personal representative on behalf of the consumer, complete the following:

### **Personal Representative:**

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Relationship to Consumer: \_\_\_\_\_

**YOU ARE ENTITLED TO A COPY OF THIS REQUEST.**

## Confidential Communication Request

### **SECTION A: Confidential communication request processing to be completed by Privacy Officer or designee.**

Date request received from consumer: \_\_\_\_/\_\_\_\_/\_\_\_\_

Date transmitted to Privacy Officer: \_\_\_\_/\_\_\_\_/\_\_\_\_

- ☐ This request is reasonable and reasonable alternative means of communication were provided. The consumer was notified on \_\_\_\_/\_\_\_\_/\_\_\_\_ by means and location appropriate to the confidentiality request that the request will be accommodated.

Departments and business associates notified to use alternative means or an alternative location to communicate about protected health information with the consumer.

\_\_\_\_\_  
\_\_\_\_\_

- ☐ This request is not reasonable and reasonable alternative means were not provided. The consumer was notified on \_\_\_\_/\_\_\_\_/\_\_\_\_ by means and location appropriate to the confidentiality request that further information is required before we can accommodate the request.

### **SIGNATURE.**

I attest that the above information is correct.

### **Privacy Officer or designee:**

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Print name: \_\_\_\_\_

Title: \_\_\_\_\_

## **ACCOMMODATION OF CONFIDENTIAL COMMUNICATION REQUEST**

**{DATE}**

**{CONSUMER'S NAME}**

**{ALTERNATIVE LOCATION ADDRESS}**

Dear **{CONSUMER}**:

This letter confirms that we will accommodate your request that we communicate about your protected health information by the alternative means or at the alternative location you requested. We will continue to use the alternative means or location you requested until further notice from you. Accordingly, please keep us informed of your need to have us communicate by the alternative means or location you requested.

If you have questions or want to discuss your request further, please contact **{CONTACT PERSON OR OFFICE}** at **{CONTACT INFORMATION}**.

Sincerely,

**{ORGANIZATION NAME}**

By: \_\_\_\_\_  
Privacy Officer or designee

**JUL 16 2003**

## DENIAL OF CONFIDENTIAL COMMUNICATION REQUEST

{DATE}

{CONSUMER'S NAME}

{ALTERNATIVE LOCATION ADDRESS}

Dear {CONSUMER}:

We are not able to accommodate your \_\_\_\_/\_\_\_\_/\_\_\_\_ request that we communicate about your protected health information by the alternative means or at the alternative location you requested. We need the following additional information before we can accommodate your request:

---

---

---

If you still want us to communicate with you about your protected health information by alternative means or location, please provide the additional information required. Until we have it, we will continue to communicate about your protected health information as follows:

---

---

---

Please contact {CONTACT PERSON OR OFFICE} at {CONTACT INFORMATION} with the additional information we need or if you have questions or want to discuss further your desire that we use confidential communications with you.

Sincerely,

{ORGANIZATION NAME}

By: \_\_\_\_\_  
Privacy Officer or designee

JUL 16 2003

## NOTIFICATION OF CONFIDENTIAL COMMUNICATION REQUIREMENT

To: {Business Associate}

From: {ORGANIZATION NAME}  
{PRIVACY OFFICER NAME AND CONTACT INFORMATION}

On \_\_\_/\_\_\_/\_\_\_, the consumer below requested that we communicate about protected health information by alternative means or at an alternative location. We are required to accommodate this request. Until further notice from us, you must adhere to the following when communicating about protected health information with this consumer:

Protected health information subject to the consumer's confidential communication request:

☐ All communications about the above protected health information must be provided to the consumer by the following means:

☐ All communications about the above protected health information must be sent to the following location:

If you have questions, please contact me.

Sincerely,  
{ORGANIZATION NAME}

By: \_\_\_\_\_  
Privacy Officer or designee

Date: \_\_\_\_\_

**Consumer requesting confidential communications:**

Name: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone: \_\_\_\_\_ Identification Number: \_\_\_\_\_

JUL 16 2003

# DATA USE AGREEMENT

This data use agreement ("Agreement") is effective upon execution, and is entered into by and between \_\_\_\_\_ ("Recipient") and Department of Mental Health, District of Columbia ("Data Provider").

Data Provider and Recipient mutually agree to enter into this Agreement to comply with the requirements of Section 514(e) of the Privacy Rule, 45 Code of Federal Regulations ("C.F.R.") § 164.514(e), issued pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as well as the District of Columbia Mental Health Information Act of 1978, DC Official Code §§ 7-1201.01 et seq. (2001).

1. **Provision of Limited Data Set.** Upon Recipient's execution of this Agreement, Data Provider will provide Recipient a Limited Data Set:
  - a) that contains the minimum amount of Protected Health Information reasonably necessary for the purposes, as set out in Section 2 of this Agreement, for which Recipient is to receive the Limited Data Set, and
  - b) from which all of the direct identifiers, as specified in 45 C.F.R. § 164.514(e)(2), of the individuals whose Protected Health Information is included in the Limited Data Set and of the relatives, household members and employers of those individuals have been removed.
2. **Recipient's Permitted Uses and Disclosures.** Recipient is permitted to use and disclose the Limited Data Set for only the following purposes (which must be limited to Health Care Operations, Public Health Activities, or Research):  
  
\_\_\_\_\_  
  
\_\_\_\_\_

There is no re-disclosure allowed by the recipient unless explicitly described as a permitted use and disclosure in this section. Any allowed re-disclosures must contain the following message:

The unauthorized disclosure of mental health information violates the provisions of the District of Columbia Mental Health Information Act of 1978. Disclosures may only be made pursuant to a valid authorization by the client, or as provided in titles III or IV of that Act. The Act provides for civil damages and criminal penalties for violations.

3. **Prohibition on Unauthorized Use or Disclosure.**
  - a) Recipient will neither use nor disclose the Limited Data Set for any purpose other than as permitted by Section 2 of this Agreement, as otherwise permitted in writing by Data Provider, or as Required by Law.
  - b) Recipient is not authorized to use or disclose the Limited Data Set in a manner that would violate the Privacy Rule, 45 C.F.R. Part 164, Subpart E, or the DC Mental Health Information Act, if done by Data Provider.
  - c) Recipient will not attempt to identify the information contained in the Limited Data Set or contact any individual who may be the subject of information contained in the Limited Data Set.
4. **Information Safeguards.** Recipient will adopt and use appropriate administrative, physical, and technical safeguards to preserve the integrity and confidentiality of the Limited Data Set and to prevent its use or disclosure, other than as permitted by Section 2 of this Agreement, as otherwise permitted in writing by Data Provider, or as Required by Law in light of the HIPAA Privacy Rules and the Mental Health Information Act.

# DATA USE AGREEMENT

**5. Permitted Recipients, Subcontractors, and Agents.** Recipient will require any agent or subcontractor, to which Recipient is permitted by this Agreement or in writing by Data Provider to disclose and let use the Limited Data Set, to agree by written contract to comply with the same restrictions and conditions that apply to Recipient's use and disclosure of the Limited Data Set pursuant to this Agreement.

In addition to Recipient, the following subcontractors, agents or other recipients are permitted to receive and use the Limited Data Set, provided that they agree to the same restrictions and conditions that apply to Recipient's use and disclosure of the Limited Data Set pursuant to this Agreement:

\_\_\_\_\_  
\_\_\_\_\_

**6. Breach of Privacy Obligations.** Recipient will report to Data Provider any use or disclosure of the Limited Data Set that is not permitted by this Agreement or in writing by Data Provider. Recipient will make the report to Data Provider's Privacy Officer within 2 days after Recipient learns of such non-permitted use or disclosure. Recipient's report will at least:

- a) Identify the nature of the non-permitted use or disclosure;
- b) Identify the Limited Data Set content used or disclosed;
- c) Identify who made the non-permitted use or disclosure and who received the non-permitted disclosure;
- d) Identify what corrective action Recipient took or will take to prevent further non-permitted uses or disclosures;
- e) Identify what Recipient did or will do to mitigate any deleterious effect of the non-permitted use or disclosure; and
- f) Provide such other information, including a written report, as Data Provider may reasonably request.

**7. Termination for Breach.** Data Provider may terminate this Agreement, and any related agreement, if it determines, in its sole discretion, that Recipient has breached any provision of this Agreement. Data Provider may exercise this termination right by providing Recipient written notice of termination that states the breach of this Agreement that provides the basis for the termination. Any such termination will be effective immediately or at such other date specified in Data Provider's notice of termination. The obligations of Section(s) 3 and 10 of this Agreement will survive termination of this Agreement.

**8. Expiration.** This Agreement will expire on \_\_\_\_\_. The obligations of Section(s) 3 and 10 of this Agreement will survive expiration of this Agreement.

**9. Return of Limited Data Set.**

- a) Upon termination or expiration of this Agreement, Recipient will, if feasible:
  - i) return to Data Provider or destroy the Limited Data Set, and
  - ii) obtain from each subcontractor, agent or other recipient, that received the Limited Data Set under Section 5 of this Agreement, the return or destruction of the Limited Data Set.

The return or destruction must include (a) the Limited Data Set, (b) all copies of the Limited Data Set, and (c) any work derived from the Limited Data Set that may allow identification of any individual whose information is contained in the Limited Data Set, in the custody or under the control of Recipient or of such subcontractor, agent or other recipient, whether in tangible or electronic medium.

## DATA USE AGREEMENT

Recipient will complete such return or destruction as promptly as possible, but not later than 20 days after the effective date of the termination or expiration of this Agreement, and will within such period certify in writing to Data Provider that such return or destruction has been completed.

b) If return or destruction is not feasible, Recipient will, within 20 days after the effective date of the termination or expiration of this Agreement:

- i) provide Data Provider with a written explanation why return or destruction is not feasible, and
- ii) certify in writing to Data Provider that Recipient, or subcontractor, agent or other recipient under Section 5 of this Agreement, will neither use nor disclose the Limited Data Set for any purpose other than the purposes that make return or destruction of the Limited Data Set infeasible.

**10. Indemnity.** Recipient will indemnify and hold harmless Data Provider and any affiliate, officer, director, employee or agent of Data Provider from and against any claim, cause of action, liability, damage, cost or expense, including attorneys' fees and court or proceeding costs, arising out of or in connection with any non-permitted use or disclosure of the Limited Data Set or other breach of this Agreement by Recipient or any subcontractor, agent, person or entity under Recipient's control.

a) **Right to Tender or Undertake Defense.** If Data Provider is named a party in any judicial, administrative or other proceeding arising out of or in connection with any non-permitted use or disclosure of the Limited Data Set or other breach of this Agreement by Recipient or any subcontractor, agent, person or entity under Recipient's control, Data Provider will have the option at any time to either (i) tender its defense to Recipient, in which case Recipient will provide qualified attorneys, consultants, and other appropriate professionals to represent Data Provider's interests at Recipient's expense, or (ii) undertake its own defense, choosing the attorneys, consultants, and other appropriate professionals to represent its interests, in which case Recipient will be responsible for and pay the reasonable fees and expenses of such attorneys, consultants, and other professionals.

b) **Right to Control Resolution.** Data Provider will have the sole right and discretion to settle, compromise or otherwise resolve any and all claims, causes of actions, liabilities or damages against it, notwithstanding that Data Provider may have tendered its defense to Recipient. Any such resolution will not relieve Recipient of its obligation to indemnify Data Provider under this Section {10}.

### 11. General Provisions.

a) **Definitions.** The terms "Health Care Operations," "Limited Data Set," "Protected Health Information," and "Research" have the meanings defined in the DMH Privacy Policies and Procedures Manual. The term "Public Health Activities" has the meaning set out in, 45 C.F.R. § 164.512(b).

b) **Amendment to Agreement.** Upon the compliance date of any final regulation or amendment to a final regulation, promulgated by the U.S. Department of Health and Human Services pursuant to the Administrative Simplification provisions of HIPAA Title II, Subtitle F, that affects Limited Data Sets, this Agreement will automatically amend such that the obligations imposed on Recipient remain in compliance with the final regulation and the Mental Health Information Act, unless either party elects to terminate this Agreement by providing written notice of termination to the other party at least 90 days before such compliance date. The obligations of Section {9} of this Agreement will apply to such termination, and the obligations of Section {s} 3 {10} of this Agreement will survive such termination.

**12. Conflicts.** The terms and conditions of this Agreement will override and control any conflicting term or condition of any other agreement between the parties to the extent that such conflicting term or condition affects Limited Data Sets.

## DATA USE AGREEMENT

IN WITNESS WHEREOF, Data Provider and Recipient execute this Agreement in multiple originals to be effective on the last date written below.

**Recipient**

**Department of Mental Health – District of Columbia**

By: \_\_\_\_\_

By: \_\_\_\_\_

Its: \_\_\_\_\_

Its: \_\_\_\_\_

Date: \_\_\_\_\_

Date: \_\_\_\_\_

# Complaint Form

**Purpose:** This form is used for a consumer to lodge a complaint about our privacy practices or compliance.

## **To the consumer lodging complaint:**

You have the right to file a complaint with us about our privacy practices or our compliance with our Privacy Practices Notice, our Privacy Policies and Procedures, or federal or DC privacy rules or law. We will investigate your complaint and provide you our written response. We will not require you to waive any right you may have under federal or DC privacy or other law to file your complaint, nor will filing your complaint adversely affect our treatment of you. To exercise this right, please complete, sign and date Sections A and B below, then submit this complaint to your agency's Privacy Officer at:

Address: \_\_\_\_\_

Telephone: \_\_\_\_\_

Fax: \_\_\_\_\_

TTD/TTY: \_\_\_\_\_ (202) 673-7500

Email: \_\_\_\_\_

If you have questions, need additional information or assistance in completing your complaint, please contact us at the above location. You may, in addition or in the alternative to filing a complaint with your agency's Privacy Officer, file a complaint with the DMH Privacy Officer, the DC Privacy Official, or the United States Department of Health and Human Services. For information on the procedures for doing that, please contact us at the above location.

## **SECTION A: Consumer lodging complaint.**

Name: \_\_\_\_\_ Maiden/Alias: \_\_\_\_\_

Address: \_\_\_\_\_

Telephone: \_\_\_\_\_ Identification Number: \_\_\_\_\_

## **SECTION B: Consumer's complaint.**

Please give a concise, plain statement of your complaint:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

## Complaint Form

Please give a concise, plain statement of the resolution you seek for your complaint:

---

---

---

---

---

---

---

**Consumer:**

I certify that the statements made in this complaint are true and correct to the best of my information and belief.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_

If this complaint is lodged by a personal representative on behalf of the consumer, complete the following:

**Personal Representative:**

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Relationship to consumer: \_\_\_\_\_

**YOU ARE ENTITLED TO A COPY OF THIS COMPLAINT.**

# Complaint Form

## COMPLAINT INVESTIGATION AND PROCESSING

Date complaint received: \_\_\_\_/\_\_\_\_/\_\_\_\_

Date complaint transmitted to Privacy Officer: \_\_\_\_/\_\_\_\_/\_\_\_\_

Investigation undertaken: \_\_\_\_\_

---

---

---

---

Findings and Conclusions: \_\_\_\_\_

---

---

---

If noncompliance found, corrective action instituted (including sanctioning any workforce member violating Privacy Policies and Procedures, Privacy Rules or other federal or DC law, and reducing any harmful effect of the noncompliance):

---

---

---

---

Report on Complaint sent on \_\_\_\_/\_\_\_\_/\_\_\_\_. Attach copy of Report on Complaint.

Matter concluded and closed on \_\_\_\_/\_\_\_\_/\_\_\_\_.

**SIGNATURE.**

I attest that the above information is correct.

**Privacy Officer or designee:**

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Print name: \_\_\_\_\_

Title: \_\_\_\_\_

## REPORT ON COMPLAINT

{DATE}

{CONSUMER'S NAME}

{CONSUMER'S ADDRESS}

Dear {CONSUMER}:

We have completed our investigation of the complaint you filed with us on \_\_\_\_/\_\_\_\_/\_\_\_\_ regarding our privacy practices or our compliance with our Joint Notice of Privacy Practices, Privacy Policies and Procedures or federal or DC privacy law. We have concluded that your complaint {has merit/is without merit} for the following reasons:

---

---

---

---

---

\_\_\_ Because we found no merit in your complaint, we are closing our file on the matter without further action.

\_\_\_ We have implemented the following corrective action to resolve the matters about which you complained:

---

---

---

If you are dissatisfied with our resolution of your complaint, you may complain to the U.S. Department of Health and Human Services. Please contact {CONTACT PERSON OR OFFICE} at {CONTACT INFORMATION} if you want information on the procedures for complaining to the U.S. Department of Health and Human Services, or if you have questions or want to discuss further our resolution of your complaint.

Sincerely,

{ORGANIZATION NAME}

By: \_\_\_\_\_  
Privacy Officer or designee

JUL 16 2003

## ASSURANCE OF PRESERVATION OF THE CONFIDENTIALITY AND SECURITY OF PROTECTED HEALTH INFORMATION

*Protected health information (PHI)* means any written, recorded, or oral information which either (1) identifies, or could be used to identify, a consumer; or (2) relates to the physical or mental health or condition of a consumer, provision of health care to a consumer, or payment for health care provided to a consumer.

District of Columbia and federal laws require that PHI of all present and former consumers be kept confidential, subject to specific allowable uses and disclosures, and that PHI be appropriately safeguarded from unauthorized access.

I understand that I hold a position of trust relative to PHI owned and/or maintained by the District of Columbia in all formats and computer systems and I have a responsibility to preserve the confidentiality and security of such information.

Accordingly, I understand that I am prohibited from engaging in inappropriate conduct, which may include, but is not limited to, the types of actions listed below:

Inappropriate discussion or display of PHI in public areas.

Failing to safeguard physical locations where PHI is available.

Failing to safeguard PHI that is carried or maintained in my possession.

Knowingly gaining, attempting to gain, causing access to, or permitting unauthorized use of or disclosure of any PHI owned and/or maintained by the District of Columbia in all formats and computer systems.

Using, attempting to use, causing or permitting the use of PHI owned and/or maintained by the District of Columbia in all formats and computer systems for personal gain or motive.

Knowingly including or causing to be included any false, inaccurate, or misleading entry into any publicly funded computer system.

Removing or causing to be removed, without proper reason and authorization, any necessary and required information owned and/or maintained by the District of Columbia in all formats and computer systems.

Abiding, abetting, or acting in conspiracy with another to violate this agreement.

Divulging my access codes to anyone.

I have been trained on and agree to adhere to all applicable policies and procedures regarding the protection of PHI.

**I acknowledge that I have signed two copies of this agreement and have received one copy for my personal information and guidance.**

Name of Employee: Please <u>print</u>	
Signature of Employee	Date
Organization/Program	
Signature of Witness	Date

Any unauthorized or inappropriate use of PHI owned and/or maintained by the District of Columbia in all formats and computer systems, by the user or by another who has inappropriately been permitted or enabled access to the system by the user, may subject the user to criminal and civil sanctions pursuant to federal and state law as well as disciplinary action up to and including removal.

## SPECIAL CONTRACT REQUIREMENTS

(Language in this appendix shall be included in or appended to all Business Associate Contracts)

### PRIVACY COMPLIANCE CLAUSE

#### (1) Definitions

(a) *Business Associate*. "Business Associate" shall mean [Insert Name of Contractor].

(b) *Covered Entity*. "Covered Entity" shall mean [Insert Name of District of Columbia Agency].

(c) *Designated Record Set* means:

1. A group of records maintained by or for Covered Entity that is:

(i) The medical records and billing records about individuals maintained by or for a covered health care provider;

(ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

(iii) Used, in whole or in part, by or for Covered Entity to make decisions about individuals.

2. For purposes of this paragraph, the term *record* means any items, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used, or disseminated by or for Covered Entity.

(d) *Individual* shall have the same meaning as the term "individual" in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

(e) *Privacy Rules*. "Privacy Rules" shall mean the requirements and restrictions contained in Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E, except to the extent District of Columbia laws (in particular, the Mental Health Information Act of 1978) have preemptive effect by operation of 45 CFR part 160, subpart B.

(f) *Protected Health Information*. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

(g) *Required By Law*. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR 164.501, except to the extent District of Columbia laws (in particular, the Mental Health Information Act of 1978) have preemptive effect by operation of 45 CFR part 160, subpart B.

JUL 1 6 2003

(h) *Secretary*. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

(2) Obligations and Activities of Business Associate

(a) Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by this Privacy Compliance Clause (this Clause) or as Required By Law.

(b) Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Clause.

(c) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Clause.

(d) Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Clause of which it becomes aware.

(e) Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

(f) Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner [Insert negotiated terms for access], to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR 164.524.

(g) Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity or an Individual, and in the time and manner [Insert negotiated terms for amendment].

(h) Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity, available to the Covered Entity, or to the Secretary, in a time and manner [Insert negotiated terms for access] or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rules.

(i) Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

(j) Business Associate agrees to provide to Covered Entity or an Individual, in time and manner [Insert negotiated terms for access], information collected in accordance with Section (i) above, to permit Covered Entity to respond to a request by an Individual for

JUL 16 2003

an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

**(3) Permitted Uses and Disclosures by Business Associate**

*(a) Refer to underlying services agreement:*

Except as otherwise limited in this Clause, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in [Insert Name of this Contract], provided that such use or disclosure would not violate the Privacy Rules if done by Covered Entity or the minimum necessary policies and procedures of Covered Entity.

(b) Except as otherwise limited in this Clause, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

(c) Except as otherwise limited in this Clause, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(d) Except as otherwise limited in this Clause, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 42 CFR 164.504(e)(2)(i)(B).

(e) Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with § 164.502(j)(1).

**(4) Obligations of Covered Entity**

(a) Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.

(b) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

(c) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

**JUL 16 2003**

**(5) Permissible Requests by Covered Entity**

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rules if done by Covered Entity.

**(6) Term and Termination**

(a) *Term.* The requirements of this Privacy Compliance Clause shall be effective as of the date of contract award, and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

(b) *Termination for Cause.* Upon Covered Entity's knowledge of a material breach of this Clause by Business Associate, Covered Entity shall either:

(1) Provide an opportunity for Business Associate to cure the breach or end the violation and terminate the contract if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

(2) Immediately terminate the contract if Business Associate has breached a material term of this Privacy Compliance Clause and cure is not possible; or

(3) If neither termination nor cure are feasible, Covered Entity shall report the violation to the Secretary.

(c) *Effect of Termination.*

(1) Except as provided in paragraph (2) of this section, upon termination of the contract, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

(2) In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon determination by the Contracting Officer that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

**(7) Miscellaneous****JUL 16 2003**

(a) *Regulatory References.* A reference in this Clause to a section in the Privacy Rules means the section as in effect or as amended.

(b) *Amendment.* The Parties agree to take such action as is necessary to amend this Clause from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rules.

(c) *Survival.* The respective rights and obligations of Business Associate under Section (6) of this Clause and Sections 9 and 20 of the Standard Contract Provisions for use with District of Columbia Government Supply and Services Contracts, effective April 2003, shall survive termination of the contract.

(d) *Interpretation.* Any ambiguity in this Clause shall be resolved to permit Covered Entity to comply with the Privacy Rules.

**JUL 16 2003**

**Department of Mental Health  
Designated Record Sets**

DATA	OWNER OF DATA / CONTACT FOR REVIEW	LOCATION OF RECORD / DATA	PAPER	ELECTRONIC	BASIC CONTENT
<b>Authority</b>					
Claims	Fiscal Policy	eCura	X	X	Demographics, diagnoses, charges for services
Claims Adjudication Records	Fiscal Policy / Care Coordination	eCura		X	Documentation of claims payments, write offs, etc.
eCura	Fiscal Policy / Care Coordination	Claims / I.S. /Access Help Line	X	X	Demographic information, authorization history, types of treatments, enrollment and transfer status, hospitalization history, and referrals for non-MHRS services.
Eligibility Information	Care Coordination	eCura	X	X	Medicaid, ACEDS download
Enrollment Records for health plans - clients	Fiscal Policy / Care Coordination	eCura / IRIS / Access Help Line	X	X	Demographic information regarding which service provider was requested
Program Record (Active Patient)	Care Coordination	eCura / IRIS	X		Face sheet of IRP / ISSP, Risk and Resiliency Information
<b>CSA</b>					
Active Record (Blue Record) - Active Patient	CSA/Medical Records Administrator	CSA Program Sites	X		1-36 months of the most current medical and programming information, discharge summary, evaluations, referrals, info from other healthcare providers
Anasazi	Anasazi/Chief Information Officer/MIS System(coming 9/03)	All Sites	X	X	Demographics, movements, Medicare #s
Appointment Schedules	Anasazi/Chief Information Officer/Dir. Adult Services/Dir. Child & Youth/Dir. CPEP	Outpatient visits, dental clinic	X	X	Dates & times of appointments, services to be rendered
Apra	CSA/Director Mental Health & Addictions	1st St / CTI	X		1-36 months of the most current medical and programming information, discharge summary, evaluations, referrals, info from other healthcare providers
Claims	CSA/CFO	Howard Road		X	Demographics, diagnoses, charges for services
Claims Adjudication Records	CSA/CFO	Howard Road		X	Documentation of claims payments, write offs, etc.

DATA	OWNER OF DATA / CONTACT FOR REVIEW	LOCATION OF RECORD / DATA	PAPER	ELECTRONIC	BASIC CONTENT
Client Master File	Anasazi/Program Mgr./Chief Infor. Officer/Dir. Child & Youth/Dir. Adult Ser./Dir. CPEP	Howard Road	X	X	Demographics on individuals, movements, diagnoses, team meeting schedules
CPEP	CSA/Director CPEP	CPEP	X		Program information and restraint records regarding the client's care while at CPEP. This may include some previous inpatient as well as outpatient information. One record per visit.
Eligibility Information	Provider Connect	64 New York Ave.	X	X	eCura @ Authority
Medical Record - OVERFLOW (Discharged Patient)	CSA/Medical Records Administrator	Programs, Spring Rd, Med Records Office, SEH Med. Rec.	X		All medical information and medication administration records regarding the client's care while at CSA. This may included previous inpatient as well as outpatient information.
Medical Record - OVERFLOW (Active Patient)	CSA/Medical Records Administrator	All CSA Program sites, Spring Road Med. Rec., CPEP	X		Medical information, on active clients, that has been purged from the active record. Information is normally more than 24 months old.
Statements	CSA/CFO	Howard Road	X	X	
<b>SEH</b>					
Medical Record (Active Patient)	Director of Medical Records	Nursing Units/Medical Records Department	X		1-12 months of the most current medical information
Assessments	Director of Medical Records	Nursing Units/Medical Records Department	X		1-12 months of the most current medical information
Claims	Patient Financial Services Manager	Barton Hall	X	X	Demographics, diagnoses, charges for services
Claims Adjudication Records	Patient Financial Services Manager	Barton Hall	X	X	Documentation of claims payments, write offs, etc.
Copies of records from other health care providers (normally included in medical or program record)	Director of Medical Records	Medical Record	X		Discharge summaries, evaluations, correspondence, medical histories, Interdisciplinary Recovery Plan Assessments

DATA	OWNER OF DATA / CONTACT FOR REVIEW	LOCATION OF RECORD / DATA	PAPER	ELECTRONIC	BASIC CONTENT
Dental	Director of Medical Records / Dental Director	In the Medical Record	X		Written notes and documentation regarding dental care.
Diagnostic Record	Director of Medical Records	In the Medical Record	X		EKG Reports
Eligibility Information	Patient Financial Services Manager	ACEDS/ Medicare Software		X	Patient Name, Social Security Number, and Date of Birth, all demographic information and benefits.
Medic Alerts	Director of Medical Records	In the Medical Record	X		Documents allergies, medical conditions, and precautions (alcohol, drug abuser)
Medical Record (Active Overflow)	Director of Medical Records	Nursing Units/Medical Records Department	X		Medical information, on active clients, that has been purged from the active record. Information is normally more than 12 months old.
Medical Record (Discharged Patient)	Director of Medical Records	Medical Records Department- 6 years most current information. Federal Repository - for information more than 7 years past current date	X		All medical information and medication administration records regarding the client's care while at SEH. This may included previous inpatient as well as outpatient information.
Medication Administration	Director of Medical Records	In the Medical Record	X		Documents medication dosages given to the patient.
Physician's Orders	Director of Medical Records	In the Medical Record	X		Physician Orders for patient care.
Podiatry	Director of Medical Records	In the Medical Record	X		Information generated by the Podiatrist
Progress Notes	Director of Medical Records	In the Medical Record	X		Physician's note with the current status of the patient's progress.
Treatment Plans/Interdisciplinary Recovery Plan	Director of Medical Records	In the Medical Record	X		The plan of care for the patient